Altitude^{TM} 4700 Series Access Point Product Reference Guide, Software Version 4.1

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800

http://www.extremenetworks.com

Published: March 2011
Part Number: 100382-00 Rev 01

Specifications are subject to change without notice.

Table of Contents

About This Guide

Introduction

This guide provides configuration and setup information for the Extreme Networks® Altitude™ 4710 dual-radio Access Point and Altitude 4750 tri-radio Access Point.

For the purposes of this guide, the devices will be called the generic term "Access Point" when identical configuration activities are applied to both models. When *command line interface* (CLI) commands are displayed, and apply to both models, an "AP4700" convention is used.

Document Conventions

The following document conventions are used in this document:

NOTE

Indicates tips or special requirements.

CAUTION

Indicates conditions that can cause equipment damage or data loss.

WARNING!

Indicates a condition or procedure that could result in personal injury or equipment damage.

Notational Conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents.
- Bullets (•) indicate:
  - action items
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
- Sequential lists (those describing step-by-step procedures) appear as numbered lists.

1 CHAPTER Introduction

As a standalone Access Point, the Altitude 4700 Series Access Point provides small and medium-sized businesses with a consolidated wired and wireless networking infrastructure, all in a single device. The integrated router, gateway, firewall, DHCP and AAA RADIUS servers, VPN, hot-spot gateway and *Power-over-Ethernet* (PoE) simplify and reduce the costs associated with networking by eliminating the need to purchase and manage multiple pieces of equipment.

The Access Point is also designed to meet the needs of large, distributed enterprises by converging the functionality of a thick Access Point and thin Access Port into a single device. This mode enables the deployment of a fully featured intelligent Access Point that can be centrally configured and managed via an Extreme Networks wireless controller in either corporate headquarters or a *network operations center* (NOC). In the event the connection between the Access Point and the wireless controller is lost, a *Remote Site Survivability* (RSS) feature ensures the delivery of uninterrupted wireless services at the local or remote site. All traffic between the adaptive Access Points and the wireless controller is secured though an IPSec tunnel. Additionally, compatibility with Extreme Networks *Wireless Management Suite* (WMS) allows you to centrally plan, deploy, monitor and secure large deployments.

The Altitude 4750 Access Points support the same feature set and firmware as the Altitude 4710 model Access Points, however Altitude 4750 Access Points support three radios (with the third radio dedicated exclusively for sensor support). For more information on the three radio Altitude 4750, see “IP Filtering” on page 38.

NOTE

Both the Altitude 4710 and Altitude 4750 model Access Points share the same Web applet (user interface) and installation methods. Therefore, the UI and installation descriptions within this guide apply to both models. There are instances where this common interface is used differently to configure various features (radio configuration, power management, and so forth), however those differences are carefully noted.

If you are new to using an Access Point for managing your network, refer to “Theory of Operations” on page 39 for an overview on wireless networking fundamentals.

New Features

The following features are now available with the introduction of the new 4.1 Altitude 4700 hardware and firmware baseline:

- Power Management Antenna Configuration File on page 18
- Hotspot Customization on page 19
- WAN Failover on page 19
- Proxy ARP Support on page 20
- Multi Cipher Support on page 20
- Dynamic Chain Selection on page 20
- Broadcast/Multicast Transmit Rate Control on page 21
- Dedicated Sensor Support on page 21
- LED Disable on page 21

Power Management Antenna Configuration File

With this most recent release of the Access Point firmware, a *Power Management Antenna Configuration File* (PMACF) has been added to the Access Point firmware that automatically configures the Access Point's radio transmit power based on the antenna type deployed, its supported gain and the deployed country's regulatory domain restrictions. The antenna type is defined using the Access Point's CLI by assigning a numerical code representing a particular type (or category) of antenna. The following are the numerical codes representing available antenna types: 0-Default antenna, 1-Dual band antenna, 2-Omni antenna, 3-Yagi antenna, 4-Embedded antenna, 5-Panel antenna, 6-Patch antenna and 7-Sector antenna. The antenna gain can be defined using either the Access Point's CLI, applet or SNMP interfaces.

Once the antenna type and gain are provided, the Access Point calculates the power range. The PMACF contains transmit power data for each Extreme Networks approved antenna type. Professional installers enter the antenna type (using the Access Point's CLI interface), and the Access Point firmware calculates the transmit power automatically. Therefore, professional installers no longer need to second guess whether the power is over the maximum allowed level.

NOTE

The antenna type and antenna gain values are maintained by the Access Point after a power cycle, and are available in imported or exported configurations.

For information on specifying the antenna type and gain for the 2.4 and 5 GHz radios using the access point CLI, see "AP4700>admin(network.wireless.radio.802-11n[2.4 GHz])>set" on page 396 for the access point's 2.4 GHz radio and "AP4700>admin(network.wireless.radio.802-11n[5.0 GHz])>set" on page 409 for the access point's 5 GHz radio.

For information on defining the antenna gain using the Access Point's GUI applet, see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174.

Hotspot Customization

To date, the default hotspot supported on the Access Point does not allow users to change the text on the hotspot portal or the logo for the enterprise where the hotspot is deployed. With this most recent release of the Access Point firmware, users now have the ability to customize the appearance of an Access Point's WLAN hotspot pages. The Access Point's hotspot feature is supported by three customer accessible pages (login page, welcome page and failure page) displayed on the client attempting to access the AP's supported hotspot. These three pages can be unique to each hotspot supported by one of the Access Point's 16 WLANs. The content of the three hotspot pages can be customized by:

- Altering the text that displays on the screen
- Altering the properties of various screen elements (such as background colors, banner and logos)
- Configuring a *cascading style sheet* (css) to define how hotspot pages display font usage, text size etc.

NOTE

The Access Point allows two logos to be displayed per page. The user has the ability to alter logo placement and screen banner color schemes.

For information on customizing a WLAN's hotspot display, see "Customizing a Hotspot Display" on page 165.

For information on the Access Point's existing (default) hotspot functionality, see "Hotspot Support" on page 35.

WAN Failover

With this most recent release of the access point firmware, a WAN failover feature has been introduced in the AP4710 access point to allow failover from the primary wired WAN connection to a 3G WAN connection. Since a 3G cellular network infrastructure is completely separate from the access point's wired infrastructure, such a wired WAN to 3G WAN failover feature assures high availability of the WAN access.

A WWAN card is a specialized network interface card, allowing a network device to connect, transmit and receive data over a cellular WAN. The WWAN card uses *point to point protoco*l (PPP) to connect to an *Internet Service Provider* (ISP) and access the Internet. PPP is the protocol used for establishing internet links over dial-up modems, DSL connections, and many other types of point-to-point links.

The wired WAN is the primary WAN link for an Altitude 4710, as long as it is enabled and connected, and the wireless WAN interface is the secondary link. For a WWAN to be a WAN or LAN recovery solution, the Altitude 4710 needs to monitor the link status of the wired WAN and actively check the health of the WAN connection. If a wired WAN or LAN connection failure is detected, an Altitude 4710 immediately establishes the WWAN connection and updates the default gateway to the WWAN interface.

The WWAN card is detected automatically when inserted into the Altitude 4710 express card slot. The card is detected as a USB/Serial device once its modules are loaded. If the card is inserted before or during module installation, the user has to wait until all the modules are loaded before the card is operational. These modules are loaded when the Altitude 4710 boots up (at runtime). Activate and configure the WWAN card from the Access Point's applet and CLI.

For more information on configuring WAN failover support, see "Configuring WAN Settings" on page 135.

Proxy ARP Support

With this most recent release of the Access Point firmware, the Access Point can respond to ARP requests on behalf of an associated MU and protect the MU's network credentials from being broadcasted on a publicly accessible network.

When Proxy ARP is enabled on the Access Point (it's enabled by default), the Access Point can make an MU physically located on one network appear part of a different network connected to the same Access Point. Proxy AP allows the Access Point to "hide" an MU's IP address behind the Access Point's firewall, while still having the MU appear to be on the public network. Proxy ARP supports both strict and dynamic modes on the Access Point.

For example, when Proxy ARP is enabled on the Access Point (it's disabled by default) and the Access Point receives an ARP request (either a wired or wireless request) for the IP address of an associated MU, the Access Point responds directly to the request (on behalf of the MU) instead of broadcasting the ARP request over the publicly accessible wireless network.

When enabled, any system on the wireless network that ARPs for the IP address of an associated MU will receive an ARP reply from the Access Point stating the requesting system should be sending packets destined for the MU to Access Point instead. In turn, the Access Point forwards the requesting packets to the target MU. Through this process, the Access Point can pass ARP requests in both directions, making an MU appear to be connected to a public network even though it's on a private network hidden behind the Access Point.

For detailed information on configuring Proxy AP support of the Access Point, see "Enabling Wireless LANs (WLANs)" on page 146.

Multi Cipher Support

Beginning with this release, professional installers have the option of deploying both new and legacy MUs within the same WLAN. Multi cipher support extends the Access Point's existing WLAN security options by allowing dynamic WEP and 802.11i configurations to co-exist, and allowing multiple security policies to be associated with the same ESSID on different WLANs. Within such an environment, legacy MUs are capable of WEP, while new MUs are capable of WPA/2-TKIP and WPA2-CCMP encryption. This particular form of multi cipher (security) support helps maintain the co-existence of dynamic WEP and 802.11i based environments.

For information on configuring Multi Cipher support, see "Configuring Multi Cipher Support" on page 216.

Dynamic Chain Selection

When enabled, dynamic chain selection forces an Access Point radio to transmit packets using legacy transmit rates (11b, 11g and/or 11a rates) using a single transmit chain. Transmissions utilizing 11n rates (MCS0–MCS15) continue to use a normal number of transmit chains, which may be 1, 2, or 3 depending on the configuration and power source. If dynamic chain selection is disabled, all transmissions utilize the same number of transmit chains. This feature is disabled by default.

NOTE

Some of the legacy 802.11abg-based devices (such as some VoWiFi phones) do not receive frames transmitted by an AP4700 series access point very well if all three transmit chains are used. When only a single transmit chain is used, communication between the access point and those client devices works better.

For information on enabling dynamic chain selection using the Access Point Web applet, see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174.

For information on using the CLI to set the access point's dynamic chain selection configuration, see "AP4700>admin(network.wireless.radio.802-11n[2.4 GHz])>set" on page 396 for the access point's 2.4 GHz radio and "AP4700>admin(network.wireless.radio.802-11n[5.0 GHz])>set" on page 409 for the access point's 5 GHz radio.

Broadcast/Multicast Transmit Rate Control

Beginning with this release, professional installers now have the ability to define the Access Point's broadcast/multicast transmission configuration. Traditionally, the Access Point used the lowest basic rate for broadcast/multicast transmissions, which was ideal from a range perspective (and remains the default configuration).

The new enhancement provides an option to increase performance by transmitting broadcast/multicast group packets at a higher rate (based on the radio's defined basic data rates). This option is optimal in environments where the Access Point's broadcast/multicast (group packet) transmission range is secondary to performance. Broadcast/multicast rate control is configurable from the Access Point's GUI applet, CLI and SNMP interfaces.

For information on configuring broadcast/multicast transmit rate control, see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174.

Dedicated Sensor Support

The Access Point supports a CLI command enabling an Access Point radio to convert to sensor only support. When enabled, only sensor mode radio configurations are permitted. Radio configurations supporting data (WLAN) support are not configurable using the Access Point's GUI, CLI or SNMP interfaces.

LED Disable

Through extensive field research, Extreme Networks has learned that not all customers wish to deploy an Access Point with blinking LEDs. Health care deployments in particular have requested an option to disable blinking LEDs. The Altitude 4700 Access Point firmware contains an option to disable blinking LEDs. The LEDs display and blink default until the disable option is invoked.

For information on disabling the Access Points LEDs, refer to "Configuring System Settings" on page 78.

LLDP Support

Linked Layer Discovery Protocol (LLDP) is a Layer 2 protocol (IEEE standard 802.1AB) used to determine the capabilities of devices such as repeaters, bridges, access points, routers and wireless clients. LLDP enables devices to advertise their capabilities and media-specific configurations.

LLDP provides a method of discovering and representing the physical network connections of a given network management domain. The LLDP neighbor discovery protocol allows you to discover and maintain accurate network topologies in a multi-vendor environment.

For more information on LLDP and its configuration, see "Configuring LLDP Settings" on page 108.

Feature Overview

The following legacy features have been carried forward into the 4.x firmware baseline:

- 802.11n Support on page 23
- Sensor Support on page 23
- Mesh Roaming Client on page 25
- Separate LAN and WAN Ports on page 25
- Multiple Mounting Options on page 26
- Antenna Support for 2.4 GHz and 5 GHz Radios on page 26
- Sixteen Configurable WLANs on page 26
- Support for 4 BSSIDs per Radio on page 26
- Quality of Service (QoS) Support on page 27
- Industry Leading Data Security on page 27
- VLAN Support on page 30
- Multiple Management Accessibility Options on page 31
- Updatable Firmware on page 31
- Programmable SNMP v1/v2/v3 Trap Support on page 31
- Power-over-Ethernet Support on page 31
- MU-MU Transmission Disallow on page 32
- Voice Prioritization on page 32
- Support for CAM and PSP MUs on page 32
- Statistical Displays on page 33
- Transmit Power Control on page 33
- Advanced Event Logging Capability on page 33
- Configuration File Import/Export Functionality on page 33
- Default Configuration Restoration on page 33
- DHCP Support on page 34
- Mesh Networking on page 34
- Additional LAN Subnet on page 35
- On-board RADIUS Server Authentication on page 35
- Hotspot Support on page 35

- Routing Information Protocol (RIP) on page 36
- Manual Date and Time Settings on page 36
- Dynamic DNS on page 36
- Auto Negotiation on page 36
- Adaptive AP on page 36
- Rogue AP Detection Enhancement on page 37
- RADIUS Time-Based Authentication on page 37
- QBSS Support on page 37
- Triple Radio Support on page 37
- IP Filtering on page 38
- MU Rate Limiting on page 38
- Per Radio MU Limit on page 38
- Power Setting Configuration on page 38
- AMSDU Transmission Support on page 39
- IPSec VPN Support on page 39

802.11n Support

Extreme Networks provides full life-cycle support for either a new or existing 802.11n mobility deployment, from network design to day-to-day support. For information on deploying your 802.11n radio, see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174.

Sensor Support

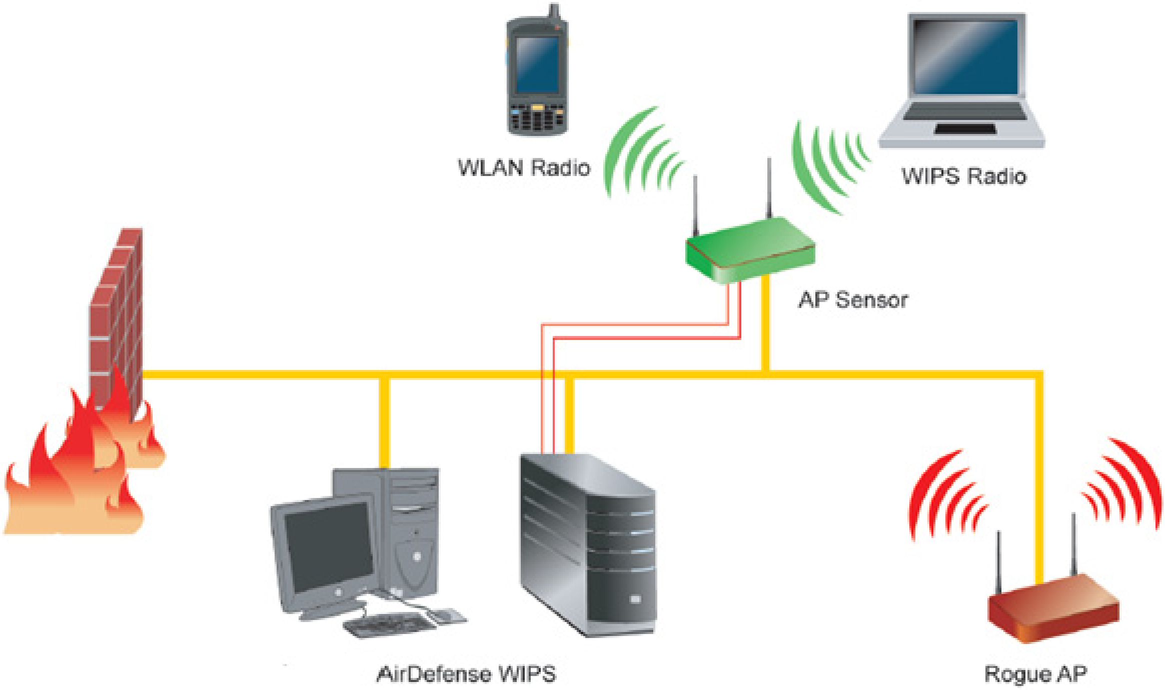
The *Wireless Intrusion Protection System* (WIPS) protects your wireless network, mobile devices and traffic from attacks and unauthorized access. WIPS provides tools for standards compliance and around-the-clock 802.11a/b/g wireless network security in a distributed environment. WIPS allows administrators to identify and accurately locate attacks, rogue devices and network vulnerabilities in real time and permits both a wired and wireless lockdown of wireless device connections upon acknowledgement of a threat.

An Access Point radio can function as a sensor and upload sensor mode operation information to a dedicated WIPS server. WIPS is not supported on a WLAN basis, rather sensor functionality is supported on the Access Point radio(s) available to each WLAN. When an Access Point radio is functioning as a WIPS sensor, it is able to scan in sensor mode across all channels within the 2.4 and 5.0 GHz bands.

NOTE

Sensor support requires a Motorola AirDefense WIPS Server on the network. Sensor functionality is not provided by the Access Point alone. The Access Point works in conjunction with a dedicated WIPS server.

The following is a network topology illustrating how a sensor functions within an Access Point supported wireless network:



A radio in sensor mode supports the following basic features:

NOTE

The functions described below are conducted on the WIPS server side, not on the Access Point.

- *Wireless Termination*—The Access Point attempts to force an unwanted (or unauthorized) connection to disconnect.
- *Wireless Sniffing*—All received frames are reported to the WIPS server. This feature provides the WIPS server with visibility into the activity on the wireless network. The WIPS server processes the received traffic and provides the IT administrator with useful information about the 802.11 RF activities in the enterprise.
- *Spectrum Analysis*—The data needed to provide the current RF Spectrum is provided to the WIPS server. The Access Point does not display the data, but it is available to the WIPS server. Spectrum analysis can operate only when there are no WLAN radios configured. The WIPS daemon and server are responsible for limiting operation only when there is no radio in WLAN mode. When a configuration change is made at the AP, the Spectrum Analysis operation stops.
- *Live View*—The WIPS application provides a live view of the sensors, APs and MUs operating in a WLAN. Live view support exists throughout the WIPS application, wherever a device icon appears in an information panel or navigation tree. Access Live View by right-clicking on the device, which automatically limits the data to the specific device your choose.

Sensor radios can be tuned to channels in both the 2.4GHz and 5.0 GHz band. The channels in use by a given radio are defined by the WIPS application. There is no need to explicitly set a band for a sensor radio. Instead, select either default values or specific channels. Specific channels can be in either band.

NOTE

Altitude 4750 models never dedicate the third radio to traditional WLAN support. The third radio is either disabled or set exclusively to WIPS support (referred to in the Access Point interface as sensor mode).

CAUTION

Users cannot define a radio as a WIPS sensor when one of the Access Point radios is functioning as a rogue AP detector. To use one of the radios as a WIPS sensor, you must disable its current detector method(s) first, then set the radio for WIPS sensor support. For information on disabling rogue AP detection, see "Configuring Rogue AP Detection" on page 243.

WIPS functionality is defined as part of the Access Point's quick setup procedure. For information on using the Access Point's Quick Setup screen to define how WIPS can be supported on an Access Point radio, see "Configuring Device Settings" on page 67.

Mesh Roaming Client

Enable the Mesh Roaming Client feature (using the Access Point's CLI) to allow a client bridge to associate in the same manner as a regular mesh client bridge. After an initial (single) association, the client bridge will not attempt additional associations. Since STP will be disabled, the association forwards data as soon as the association attempt is successful. When Mesh Roaming Client is enabled, base bridge mode is not supported to avoid a loop within the mesh topology. Thus, the Mesh Roaming Client is always an end point (by design) within the mesh wireless topology. The base bridge will need STP disabled to immediately begin forwarding data when a roaming client bridge associates.

Separate LAN and WAN Ports

The Access Point has one LAN (GE1/POE) port and one WAN (GE2) port, each with their own MAC address. The Access Point must manage all data traffic over the LAN connection carefully as either a DHCP client, BOOTP client, DHCP server or using a static IP address. The Access Point can only use a Power-over-Ethernet device when connected to the LAN port.

For detailed information on configuring the LAN port, see "Configuring the LAN Interface" on page 123.

A *Wide Area Network (WAN)* is a widely dispersed telecommunications network. In a corporate environment, the WAN port might connect to a larger corporate network. For a small business, the WAN port might connect to a DSL or cable modem to access the Internet. Regardless, network address information must be configured for the Access Point's intended mode of operation.

For detailed information on configuring the Access Point's WAN port, see "Configuring WAN Settings" on page 135.

The LAN and WAN port MAC addresses can be located within the LAN and WAN Stats screens.

For detailed information on locating the Access Point's MAC addresses, see "Viewing WAN Statistics" on page 263 and "Viewing LAN Statistics" on page 266. For information on Access Point MAC address assignments, see "MAC Address Assignment" on page 43.

Multiple Mounting Options

The access point attaches to a wall, mounts under a ceiling or above a ceiling (attic). Choose a mounting option based on the physical environment of the coverage area. Do not mount the Access Point in a location that has not been approved in a radio coverage site survey.

For detailed information on the mounting options available , see "Mounting an Altitude 4700 Series Access Point" on page 50.

Antenna Support for 2.4 GHz and 5 GHz Radios

The Access Point supports several 802.11a/n and 802.11b/g/n radio antennas. Select the antenna best suited to the radio transmission requirements of your coverage area.

For a comprehensive overview of the antennas and associated components supported by the Extreme Networks access point family, see the *Altitude 35xx/46xx/47xx AP Antenna Selection Guide, Rev.xx*.

Sixteen Configurable WLANs

A *Wireless Local Area Network (WLAN)* is a data-communications system that flexibly extends the functionalities of a wired LAN. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one Access Point to another like a cellular phone system. WLANs can therefore be configured around the needs of specific groups of users, even when they are not in physical proximity. Sixteen WLANs are configurable on each Access Point.

To enable and configure WLANs on an Access Point radio, see "Enabling Wireless LANs (WLANs)" on page 146.

Support for 4 BSSIDs per Radio

The Access Point supports four BSSIDs per radio. Each BSSID has a corresponding MAC address. The first MAC address corresponds to BSSID #1. The MAC addresses for the other three BSSIDs (BSSIDs #2, #3, #4) are derived by adding 1, 2, 3, respectively, to the radio MAC address.

If the radio MAC address displayed on the Radio Settings screen is 00:23:68:72:20:DC, then the BSSIDs for that radio will have the following MAC addresses:

BSSID	MAC Address	Hexadecimal Addition
BSSID #1	00:23:68:72:20:DC	Same as Radio MAC address
BSSID #2	00:23:68:72:20:DD	Radio MAC address +1
BSSID #3	00:23:68:72:20:DE	Radio MAC address +2
BSSID #4	00:23:68:72:20:DF	Radio MAC address +3

For detailed information on strategically mapping BSSIDs to WLANs, see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174. For information on Access Point MAC address assignments, see "MAC Address Assignment" on page 43.

Quality of Service (QoS) Support

The QoS implementation provides applications running on different wireless devices a variety of priority levels to transmit data to and from the Access Point. Equal data transmission priority is fine for data traffic from applications such as Web browsers, file transfers or email, but is inadequate for multimedia applications.

Voice over Internet Protocol (VoIP), video streaming and interactive gaming are highly sensitive to latency increases and throughput reductions. These forms of higher priority data traffic can significantly benefit from the QoS implementation.The *WiFi Multimedia QOS Extensions (WMM)* implementation used by the shortens the time between transmitting higher priority data traffic and is thus desirable for multimedia applications. In addition, U-APSD (WMM Power Save) is also supported.

WMM defines four access categories—*voice*, *video*, *best effort* and *background*—to prioritize traffic for enhanced multimedia support.

For detailed information on configuring QoS support, see "Setting the WLAN Quality of Service (QoS) Policy" on page 156.

Industry Leading Data Security

The Access Point supports numerous encryption and authentication techniques to protect the data transmitting on the WLAN.

The following authentication techniques are supported:

- Kerberos Authentication on page 27
- EAP Authentication on page 28

The following encryption techniques are supported:

- WEP Encryption on page 28
- KeyGuard Encryption on page 29
- Wi-Fi Protected Access (WPA) Using TKIP Encryption on page 29
- WPA2-CCMP (802.11i) Encryption on page 29

In addition, the Access Point supports the following additional security features:

- Firewall Security on page 30
- VPN Tunnels on page 30
- Content Filtering on page 30

For an overview on the encryption and authentication schemes available, refer to *"Configuring Access Point Security" on page 197.*

Kerberos Authentication

Authentication is a means of verifying information transmitted from a secure source. If information is *authentic*, you know who created it and you know it has not been altered in any way since it was originated. Authentication entails a network administrator employing a software "supplicant" on their computer or wireless device.

Authentication is critical for the security of any wireless LAN device. Traditional authentication methods are not suitable for use in wireless networks where an unauthorized user can monitor network traffic and intercept passwords. The use of strong authentication methods that do not disclose passwords is necessary. The Access Point uses the *Kerberos* authentication service protocol (specified in RFC 1510) to authenticate users/clients in a wireless network environment and to securely distribute the encryption keys used for both encrypting and decrypting.

A basic understanding of *RFC 1510 Kerberos Network Authentication Service (V5)* is helpful in understanding how Kerberos works. By default, WLAN devices operate in an *open system network* where any wireless device can associate with an AP without authorization. Kerberos requires device authentication before access to the wired network is permitted.

For detailed information on Kerberos configurations, see "Configuring Kerberos Authentication" on page 202.

EAP Authentication

The *Extensible Authentication Protocol (EAP)* feature provides Access Points and their associated MUs an additional measure of security for data transmitted over the wireless network. Using EAP, authentication between devices is achieved through the exchange and verification of certificates.

EAP is a mutual authentication method whereby both the MU and AP are required to prove their identities. Like Kerberos, the user loses device authentication if the server cannot provide proof of device identification.

Using EAP, a user requests connection to a WLAN through the Access Point. The Access Point then requests the identity of the user and transmits that identity to an authentication server. The server prompts the AP for proof of identity (supplied to the Access Point by the user) and then transmits the user data back to the server to complete the authentication process.

An MU is not able to access the network if not authenticated. When configured for EAP support, the Access Point displays the MU as an EAP station.

EAP is only supported on mobile devices running Windows XP, Windows 2000 (using Service Pack #4) and Windows Mobile 2003. Refer to the system administrator for information on configuring a RADIUS Server for EAP (802.1x) support.

For detailed information on EAP configurations, see "Configuring 802.1x EAP Authentication" on page 204.

WEP Encryption

All WLAN devices face possible information theft. Theft occurs when an unauthorized user eavesdrops to obtain information illegally. The absence of a physical connection makes wireless links particularly vulnerable to this form of theft. Most forms of WLAN security rely on encryption to various extents. Encryption entails scrambling and coding information, typically with mathematical formulas called *algorithms*, before the information is transmitted. An algorithm is a set of instructions or formula for scrambling the data. A *key* is the specific code used by the algorithm to encrypt or decrypt the data. *Decryption* is the decoding and unscrambling of received encrypted data.

The same device, host computer or front-end processor, usually performs both encryption and decryption. The transmit or receive direction determines whether the encryption or decryption function is performed. The device takes plain text, encrypts or scrambles the text typically by mathematically combining the key with the plain text as instructed by the algorithm, then transmits the data over the network. At the receiving end, another device takes the encrypted text and decrypts, or unscrambles, the text revealing the original message. An unauthorized user can know the algorithm, but cannot interpret the encrypted data without the appropriate key. Only the sender and receiver of the transmitted data know the key.

Wired Equivalent Privacy (WEP) is an encryption security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b and supported by the AP. WEP encryption is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN. The level of protection provided by WEP encryption is determined by the encryption key length and algorithm. An encryption key is a string of case sensitive characters used to encrypt and decrypt data packets transmitted between a mobile unit (MU) and the Access Point. An Access Point and its associated wireless clients must use the same encryption key (typically 1 through 4) to interoperate.

For detailed information on WEP, see "Configuring WEP Encryption" on page 208.

KeyGuard Encryption

Use KeyGuard to shield the master encryption keys from being discovered through hacking. KeyGuard negotiation takes place between the Access Point and MU upon association. The Access Point can use KeyGuard with certain Motorola MUs. KeyGuard is only supported on certain Motorola MUs.

For detailed information on KeyGuard configurations, see "Configuring KeyGuard Encryption" on page 209.

Wi-Fi Protected Access (WPA) Using TKIP Encryption

Wi-Fi Protected Access (WPA) is a security standard for systems operating with a Wi-Fi wireless connection. WEP's lack of user authentication mechanisms is addressed by WPA. Compared to WEP, WPA provides superior data encryption and user authentication.

WPA addresses the weaknesses of WEP by including:

- a per-packet key mixing function
- a message integrity check
- an extended initialization vector with sequencing rules
- a re-keying mechanism

WPA uses an encryption method called *Temporal Key Integrity Protocol* (TKIP). WPA employs 802.1X and *Extensible Authentication Protocol* (EAP).

For detailed information on WPA using TKIP configurations, see "Configuring WPA/WPA2 Using TKIP" on page 211.

WPA2-CCMP (802.11i) Encryption

WPA2 is a newer 802.11i standard that provides even stronger wireless security than *Wi-Fi Protected Access* (WPA) and WEP. *Counter-mode/CBC-MAC Protocol (CCMP)* is the security standard used by the *Advanced Encryption Standard (AES).* AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check (MIC)* using the proven *Cipher Block Message Authentication Code (CBC-MAC)* technique. Changing just one bit in a message produces a totally different result.

WPA2-CCMP is based on the concept of a *Robust Security Network (RSN),* which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the keys the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is an encryption scheme as secure as any the Access Point provides.

For detailed information on WPA2-CCMP, see “Configuring WPA2-CCMP (802.11i)” on page 213.

Firewall Security

A firewall keeps personal data in and hackers out. The Access Point’s firewall prevents suspicious Internet traffic from proliferating the Access Point managed network. The Access Point performs *Network Address Translation* (NAT) on packets passing to and from the WAN port. This combination provides enhanced security by monitoring communication with the wired network.

For detailed information on configuring the Access Point’s firewall, see “Configuring Firewall Settings” on page 218.

VPN Tunnels

Virtual Private Networks (VPNs) are IP-based networks using encryption and tunneling providing users remote access to a secure LAN. In essence, the trust relationship is extended from one LAN across the public network to another LAN, without sacrificing security. A VPN behaves like a private network; however, because the data travels through the public network, it needs several layers of security. The Access Point can function as a robust VPN gateway.

For detailed information on configuring VPN security support, see “Configuring VPN Tunnels” on page 225.

Content Filtering

Content filtering allows system administrators to block specific commands and URL extensions from going out through the WAN port. Therefore, content filtering affords system administrators selective control on the content proliferating the network and is a powerful screening tool. Content filtering allows the blocking of up to 10 files or URL extensions and allows blocking of specific outbound HTTP, SMTP, and FTP requests.

For detailed information on configuring content filtering support, see “Configuring Content Filtering Settings” on page 240.

VLAN Support

A *Virtual Local Area Network (VLAN)* can electronically separate data on the same AP from a single broadcast domain into separate broadcast domains. By using a VLAN, you can group by logical function instead of physical location. There are 16 VLANs supported on the Access Point. An administrator can map up to 16 WLANs to 16 VLANs and enable or disable dynamic VLAN assignment. In addition to these 16 VLANs, the Access Point supports dynamic, user-based, VLANs when using EAP authentication.

VLANs enable organizations to share network resources in various network segments within large areas (airports, shopping malls, etc.). A VLAN is a group of clients with a common set of requirements independent of their physical location. VLANs have the same attributes as physical LANs, but they enable administrators to group clients even when they are not members of the same network segment.

For detailed information on configuring VLAN support, see “Configuring VLAN Support” on page 126.

Multiple Management Accessibility Options

The Access Point can be accessed and configured using one of the following:

- Java-Based Web UI
- Human readable config file (imported via FTP or TFTP)
- MIB (Management Information Base)
- *Command Line Interface (CLI)* accessed via RS-232 or Telnet. Use the Access Point's DB-9 serial port for direct access to the command-line interface from a PC. Use a Null-Modem cable (Part No. 25-632878-0) for the best fitting connection.

Updatable Firmware

Extreme Networks periodically releases updated versions of device firmware to the Extreme Networks Web site. If the firmware version displayed on the System Settings screen (see "Configuring System Settings" on page 78) is older than the version on the Web site, Extreme Networks recommends updating the Access Point to the latest firmware version for full feature functionality.

For detailed information on updating the firmware using FTP or TFTP, see "Updating Device Firmware" on page 118.

Programmable SNMP v1/v2/v3 Trap Support

Simple Network Management Protocol (SNMP) facilitates the exchange of management information between network devices. SNMP uses *Management Information Bases (MIBs)* to manage the device configuration and monitor Internet devices in remote locations. MIB information accessed via SNMP is defined by a set of managed objects called *Object Identifiers (OIDs)*. An OID is used to uniquely identify each object variable of a MIB.

SNMP allows a network administrator to configure the Access Point, manage network performance, find and solve network problems, and plan network growth. The Access Point supports SNMP management functions for gathering information from its network components. The Access Point's download site contains the following MIB files supporting the Access Point:

- EXTR-CC-AP4700-MIB-2.0 (standard MIB file)
- EXTR-AP4700-MIB-02a02

The Access Point's SNMP agent functions as a command responder and is a multilingual agent responding to SNMPv1, v2c and v3 managers (command generators). The factory default configuration maintains SNMPv1/2c support of community names, thus providing backward compatibility.

For detailed information on configuring SNMP traps, see "Configuring SNMP Settings" on page 97.

Power-over-Ethernet Support

When users purchase an Extreme Networks WLAN solution, they often need to place Access Points in obscure locations. In the past, a dedicated power source was required for each Access Point in addition to the Ethernet infrastructure. This often required an electrical contractor to install power drops at each Access Point location.

An approved Power Injector solution merges power and Ethernet into one cable, reducing the burden of installation and allows optimal access point placement in respect to the intended radio coverage area.

The access point can only use a Power-over-Ethernet device when connected to the access point's LAN (GE1/POE) port. The access point can also support 3af/3at compliant products from other vendors.

The Power Injector (Part No. AP-PSBIAS-1P3-AFR) is a single-port Power-over-Ethernet hub combining low-voltage DC with Ethernet data in a single cable connecting to the access point. The Power Injector's single DC and Ethernet data cable creates a modified Ethernet cabling environment on the access point's LAN port eliminating the need for separate Ethernet and power cables. For detailed information on using the Power Injector, see "Power Injector System" on page 48

MU-MU Transmission Disallow

The Access Point's MU-MU Disallow feature prohibits MUs from communicating with each other even if on the same WLAN, assuming one of the WLAN's is configured to disallow MU-MU communication. Therefore, if an MU's WLAN is configured for MU-MU disallow, it will not be able to communicate with any other MUs connected to this Access Point.

For detailed information on configuring an WLAN to disallow MU to MU communications, see "Creating/Editing Individual WLANs" on page 148.

Voice Prioritization

Each Access Point WLAN has the capability of having its QoS policy configured to prioritize the network traffic requirements for associated MUs. A WLAN QoS page is available for each enabled WLAN on either the 802.11a/n or 802.11b/g/n radio.

Use the QoS page to enable voice prioritization for devices to receive the transmission priority they may not normally receive over other data traffic. Voice prioritization allows the Access Point to assign priority to voice traffic over data traffic, and (if necessary) assign legacy voice supported devices (non WMM supported voice devices) additional priority.

For detailed information on configuring voice prioritization over other voice enabled devices, see "Setting the WLAN Quality of Service (QoS) Policy" on page 156.

Support for CAM and PSP MUs

The Access Point supports both CAM and PSP powered MUs. *CAM (Continuously Aware Mode)* MUs leave their radios on continuously to hear every beacon and message transmitted. These systems operate without any adjustments by the Access Point.

A beacon is a uniframe system packet broadcast by the AP to keep the network synchronized. A beacon includes the ESSID, MAC address, Broadcast destination addresses, a time stamp, a *DTIM (Delivery Traffic Indication Message)* and the *TIM (Traffic Indication Map)*.

PSP (Power Save Polling) MUs power off their radios for short periods. When an MU in PSP mode associates with an Access Point, it notifies the Access Point of its activity status. The Access Point responds by buffering packets received for the MU. PSP mode is used to extend an MU's battery life by enabling the MU to "sleep" during periods of inactivity.

Statistical Displays

The Access Point can display robust transmit and receive statistics for the WAN and LAN ports. WLAN stats can be displayed collectively and individually for enabled WLANs. Transmit and receive statistics are available for the Access Point's 802.11a/n and 802.11b/g/n radios. An advanced radio statistics page is also available to display retry histograms for specific data packet retry information.

Associated MU stats can be displayed collectively and individually for specific MUs. An echo (ping) test is also available to ping specific MUs to assess association strength. Finally, the Access Point can detect and display the properties of other APs detected within its radio coverage area. The type of AP detected can be displayed as well as the properties of individual APs.

For detailed information on available Access Point statistical displays and the values they represent, see "Monitoring Statistics" on page 263.

Transmit Power Control

The Access Point has a configurable power level for each radio. This enables the network administrator to define the antenna's transmission power level in respect to the Access Point's placement or network requirements as defined in the site survey.

For detailed information on setting the radio transmit power level, see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174.

Advanced Event Logging Capability

The Access Point periodically logs system events. Logging events is useful in assessing the throughput and performance of the Access Point or troubleshooting problems on the Access Point managed *Local Area Network* (LAN).

For detailed information on Access Point events, see "Logging Configuration" on page 112.

Configuration File Import/Export Functionality

Configuration settings for an Access Point can be downloaded from the current configuration of another Access Point. This affords the administrator the ability to save the current configuration before making significant changes or restoring a default configuration.

For detailed information on importing or exporting configuration files, see "Importing/Exporting Configurations" on page 114.

Default Configuration Restoration

The Access Point can restore its default configuration or a partial default configuration (with the exception of current WAN and SNMP settings). Restoring the default configuration is a good way to create new WLANs if the MUs the Access Point supports have been moved to different radio coverage areas.

For detailed information on restoring a default or partial default configuration, see "Configuring System Settings" on page 78.

DHCP Support

The Access Point can use *Dynamic Host Configuration Protocol (DHCP)* to obtain a leased IP address and configuration information from a remote server. DHCP is based on the BOOTP protocol and can coexist or interoperate with BOOTP. Configure the Access Point to send out a *DHCP request* searching for a *DHCP/BOOTP* server to acquire HTML, firmware or network configuration files when the Access Point boots. Because BOOTP and DHCP interoperate, whichever responds first becomes the server that allocates information.

The Access Point can be set to only accept replies from DHCP or BOOTP servers or both (this is the default setting). Disabling DHCP disables BOOTP and DHCP and requires network settings to be set manually. If running both DHCP and BOOTP, do not select BOOTP Only. BOOTP should only be used when the server is running BOOTP exclusively.

The DHCP client automatically sends a DHCP request at an interval specified by the DHCP server to renew the IP address lease as long as the Access Point is running (this parameter is programmed at the DHCP server). For example: Windows 2000 servers typically are set for 3 days.

Mesh Networking

Utilize the new mesh networking functionality to allow the Access Point to function as a bridge to connect two Ethernet networks or as a repeater to extend your network's coverage area without additional cabling. Mesh networking is configurable in two modes. It can be set in a wireless client bridge mode and/or a wireless base bridge mode (which accepts connections from client bridges). These two modes are not mutually exclusive.

In client bridge mode, the Access Point scans to find other Access Points using the selected WLAN's ESSID. The Access Point must go through the association and authentication process to establish a wireless connection. The mesh networking association process is identical to the Access Point's MU association process. Once the association/authentication process is complete, the wireless client adds the connection as a port on its bridge module. This causes the Access Point (in client bridge mode) to begin forwarding configuration packets to the base bridge. An Access Point in base bridge mode allows the Access Point radio to accept client bridge connections.

The two bridges communicate using the *Spanning Tree Protocol* (STP). The spanning tree determines the path to the root and detects if the current connection is part of a network loop with another connection. Once the spanning tree converges, both Access Points begin learning which destinations reside on which side of the network. This allows them to forward traffic intelligently.

After the Access Point (in client bridge mode) establishes at least one wireless connection, it will begin beaconing and accepting wireless connections (if configured to support mobile users). If the Access Point is configured as both a client bridge and a base bridge, it begins accepting client bridge connections. In this way, the mesh network builds itself over time and distance.

Once the Access Point (in client bridge mode) establishes at least one wireless connection, it establishes other wireless connections in the background as they become available. In this way, the Access Point can establish simultaneous redundant links. An Access Point (in client bridge mode) can establish up to 3 simultaneous wireless connections with other Access Points. A client bridge always initiates the connections and the base bridge is always the acceptor of the mesh network data proliferating the network.

Since each Access Point can establish up to 3 simultaneous wireless connections, some of these connections may be redundant. In that case, the STP algorithm determines which links are the redundant links and disables the links from forwarding.

For an overview on mesh networking as well as details on configuring the Access Point's mesh networking functionality, see "Configuring Mesh Networking" on page 577.

Additional LAN Subnet

In a typical retail or small office environment (wherein a wireless network is available along with a production WLAN) it is often necessary to segment a LAN into two subnets. Consequently, a second LAN is required to "segregate" wireless traffic.

The Access Point has a second LAN subnet enabling administrators to segment the Access Point's LAN connection into two separate networks. The main Access Point LAN screen now allows the user to select either LAN1 or LAN2 as the active LAN over the Access Point's Ethernet port. Both LANs can still be active at any given time, but only one can transmit over the Access Point's physical LAN connection. Each LAN has a separate configuration screen (called LAN 1 and LAN 2 by default) accessible under the main LAN screen. The user can rename each LAN as necessary. Additionally, each LAN can have its own Ethernet Type Filter configuration, and subnet access (HTTP, SSH, SNMP and telnet) configuration.

For detailed information on configuring the Access Point for additional LAN subnet support, see "Configuring the LAN Interface" on page 123.

On-board RADIUS Server Authentication

The Access Point can function as a RADIUS Server to provide user database information and user authentication. Several new screens have been added to the Access Point's menu tree to configure RADIUS server authentication and configure the local user database and access policies. The new RADIUS Server functionality allows an administrator to define the data source, authentication type and associate digital certificates with the authentication scheme. The LDAP screen allows the administrator to configure an external LDAP Server for use with the Access Point. A new Access Policy screen enables the administrator to set WLAN access based on user groups defined within the User Database screen. Each user is authorized based on the access policies applicable to that user. Access policies allow an administrator to control access to a user groups based on the WLAN configurations.

For detailed information on configuring the Access Point for AAA RADIUS Server support, see "Configuring User Authentication" on page 250.

Hotspot Support

The Access Point allows hotspot operators to provide user authentication and accounting without a special client application. The Access Point uses a traditional Internet browser as a secure authentication device. Rather than rely on built-in 802.11 security features to control Access Point association privileges, you can configure a WLAN with no WEP (an open network). The Access Point issues an IP address to the user using a DHCP server, authenticates the user, and grants the user access to the Internet.

If a tourist visits a public hotspot and wants to browse a Web page, they boot their laptop and associate with a local Wi-Fi network by entering a valid SSID. They start a browser, and the hotspot's access controller forces the un-authenticated user to a Welcome page (from the hotspot operator) that allows the user to login with a username and password. In order to send a redirected page (a login page), a TCP termination exists locally on the Access Point. Once the login page displays, the user enters their credentials. The Access Point connects to the RADIUS server and determines the identity of the connected wireless user. Thus, allowing the user access to the Internet once successfully authenticated.

For detailed information on configuring the Access Point for Hotspot support, see “Configuring WLAN Hotspot Support” on page 160.

Routing Information Protocol (RIP)

RIP is an interior gateway protocol that specifies how routers exchange routing-table information. The parent Router screen also allows the administrator to select the type of RIP and the type of RIP authentication used.

For detailed information on configuring RIP functionality as part of the Access Point’s Router functionality, see “Setting the RIP Configuration” on page 187.

Manual Date and Time Settings

As an alternative to defining an NTP server to provide Access Point system time, the Access Point can now have its date and time set manually. A new Manual Date/Time Setting screen can be used to set the time using a Year-Month-Day HH:MM:SS format.

For detailed information on manually setting the Access Point’s system time, see “Configuring Network Time Protocol (NTP)” on page 110.

Dynamic DNS

The Access Point supports the Dynamic DNS service. *Dynamic DNS* (or DynDNS) is a feature offered by *www.dyndns.com* allowing the mapping of domain names to dynamically assigned IP addresses. When the dynamically assigned IP address of a client changes, the new IP address is sent to the DynDNS service and traffic for the specified domain(s) is routed to the new IP address. For information on configuring Dynamic DNS, see “Configuring Dynamic DNS” on page 145.

Auto Negotiation

Auto negotiation enables the Access Point to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when using the Access Point in an environment where different devices are connected and disconnected on a regular basis. For information on configuring the auto negotiation feature, see “Configuring the LAN Interface” on page 123 or “Configuring WAN Settings” on page 135.

Adaptive AP

An *adaptive AP* (AAP) is an Access Point that can adopt like an Altitude 4600 Access Point (L3). The management of an AAP is conducted by a controller, once the Access Point connects to an Extreme Networks controller and receives its AAP configuration.

An AAP provides:

- local 802.11 traffic termination
- local encryption/decryption
- local traffic bridging
- the tunneling of centralized traffic to the wireless controller

For a information overview of the adaptive AP feature as well as how to configure it, refer to "Adaptive AP" on page 605.

Rogue AP Detection Enhancement

The Access Point can scan for rogues over all channels on both of the Access Point's radio bands. The switching of radio bands is based on a timer with no user intervention required.

For information on configuring the Access Point for Rogue AP support, see "Configuring Rogue AP Detection" on page 243.

RADIUS Time-Based Authentication

An external server maintains a users and groups database used by the Access Point for access permissions. Various kinds of access policies can be applied to each group. Individual groups can be configured with their own time-based access policy. Each group's policy has a user defined interval defining the days and hours access is permitted. Authentication requests for users belonging to the group are honored only during these defined hourly intervals.

For more information on defining Access Point access policies by group, see "Defining User Access Permissions by Group" on page 259.

QBSS Support

Each Access Point radio can be configured to optionally allow the Access Point to communicate channel usage data to associated devices and define the beacon interval used for channel utilization transmissions. The QBSS load represents the percentage of time the channel is in use by the Access Point and the Access Point's station count. This information is very helpful in assessing the Access Point's overall load on a channel, its availability for additional device associations and multi media traffic support.

For information on enabling QBSS and defining the channel utilization transmission interval, see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174.

Triple Radio Support

The Altitude 4750 Access Points contains three radios. The third Altitude 4750 radio is never a WLAN radio. The third radio is either disabled or set to sensor mode. A radio's mode is called its RF function. By default, a radio's RF function is WLAN. A WLAN radio is a traditional Access Point radio that does not provide WIPS support. When a radio's RF function becomes WIPS, the radio takes on the role of what is typically referred to as a sensor.

NOTE

Since the only radio function allowed for the third radio is WIPS, there is no radio 3 submenu in the Access Point CLI.

NOTE

For information on setting the configuration of a three radio model Altitude 4750, see “Configuring the 802.11a/n or 802.11b/g/n Radio” on page 174.

IP Filtering

IP filtering determines which IP packets are processed normally and which are discarded. If discarded, the packet is deleted and completely ignored (as if never received). Optionally apply different criteria to better refine which packets to filter.

IP filtering supports the creation of up to 20 filter rules enforced at layer 3. Once defined (using the Access Point’s SNMP, GUI or CLI), filtering rules can be enforced on the Access Point’s LAN1, LAN2 and WLAN interfaces. An additional default action is also available denying traffic when the filter rules fail. Lastly, imported and exported configurations retain their defined IP filtering configurations.

For information on configuring the Access Point’s IP filtering functionality, see “Configuring IP Filtering” on page 188.

MU Rate Limiting

MU rate limiting enables an administrator to determine how much radio bandwidth is allocated to each MU within any one of the 16 supported WLANs.

To globally enable or disable the MU rate limit and assess the WLANs in which it’s currently invoked, see “Configuring MU Rate Limiting” on page 184.

To define the actual MU rate limit (maximum downstream bandwidth allocation in kbps), see “Creating/Editing Individual WLANs” on page 148.

Per Radio MU Limit

An Access Point can reserve slots on each radio so MUs of one radio type (11a/n or 11bg/n) have better chances for AP association. Therefore, the total number of MUs allowed to associate remains at 127, but you can now strategically distribute the 127 MU associations between the data radios.

For information on setting the number of MU associations on a specific radio, see “Configuring the 802.11a/n or 802.11b/g/n Radio” on page 174.

Power Setting Configuration

The Access Point’s power management functionality automatically configures the AP's operational mode so it safely operates within available power. The power setting feature enables the user to select one of three power operating modes, 3af, 3at and full power. When an Access Point is operating in either 3af or 3at mode, the transmit power is always lower than the full power setting. With the introduction of the Altitude 4750 model Access Point and its optional three radio SKU, the power options available amongst single, dual and three radio model Access Points has never been more diverse, and careful consideration must be made before deploying the Access Point.

The AP's hardware design uses a *complex programmable logic device* (CPLD). When an AP is powered on (or performing a cold reset), the CPLD determines the maximum power available to the AP by a POE device. Once an operational power configuration is defined, the AP firmware can read the power setting and configure operating characteristics based on the AP's SKU and power configuration. If the POE cannot provide sufficient power (with all interfaces enabled), the following interfaces could be disabled or modified:

- Radio transmit power could be reduced due to lack of sufficient power or the radio can be disabled
- The WAN port configuration could be changed (enabled or disabled)

For information on configuring the Access Point's power configuration, see "Configuring Power Settings" on page 81.

AMSDU Transmission Support

Aggregate MAC Service Data Unit (AMSDU) is an 802.11n specific MAC feature which enhances the transmission of multiple MSDU contents wrapped within a single preamble/packet infrastructure. The AMSDU transmission limit is set to 3839 bites by default.

For information on configuring AMSDU support for an Access Point radio, see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174. AMSDU support can be defined by selecting the Set Aggregation button within the *Network Configuration* > *Wireless* > *Radio Configuration* > *Radio1* screen.

IPSec VPN Support

A VPN ensures data privacy between two end points, even while using a communication medium which is itself insecure (like the Internet). VPNs create a secure tunnel between two end points as if they are directly connected over a secure connection. Traffic is secured using a robust IPSec encryption technique.

You can get the safety of a VPN in a WLAN by hosting the VPN server at the Access Point, and the VPN client software on the MU. For that reason, a VPN provides secure WLAN access to MUs. A VPN solution was more common before 802.11i was introduced, but is not as common now, since 802.11i/ WPA2 is considered more secure.

For information on configuring VPN support, see "Configuring VPN Tunnels" on page 225. For instructions on configuring a IPSec VPN tunnel using two Access Points, see "Creating a VPN Tunnel between Two Access Points" on page 229.

Theory of Operations

To understand Access Point management and performance alternatives, users need familiarity with functionality and configuration options. The Access Point includes features for different interface connections and network management.

The Access Point uses electromagnetic waves to transmit and receive electric signals without wires. Users communicate with the network by establishing radio links between *mobile units (MUs)* and Access Points.

The Access Point uses *DSSS (direct sequence spread spectrum)* to transmit digital data from one device to another. A radio signal begins with a carrier signal that provides the base or center frequency. The digital data signal is encoded onto carriers using a DSSS *chipping algorithm*. The radio signal propagates into the air as electromagnetic waves. A receiving antenna (on the MU) in the path of the waves absorbs the waves as electrical signals. The receiving MU interprets (demodulates) the signal by reapplying the direct sequence chipping code. This demodulation results in the original digital data.

The Access Point uses its environment (the air and certain objects) as the transmission medium.The Access Point can either transmit in the 2.4 to 2.5-GHz frequency range (802.11b/g/n radio) or the 5 GHz frequency range (802.11a/n radio), the actual range is country-dependent. Extreme Networks devices, like other Ethernet devices, have unique, hardware encoded *Media Access Control (MAC)* or IEEE addresses. MAC addresses determine the device sending or receiving data. A MAC address is a 48-bit number written as six hexadecimal bytes separated by colons. For example: 00:04:96:44:51:90. Also see the following:

- "Wireless Coverage"
- "MAC Layer Bridging"
- "Content Filtering"
- "DHCP Support"
- "Media Types"
- "Direct-Sequence Spread Spectrum"
- "MU Association Process"
- "Operating Modes"
- "Management Access Options"
- "MAC Address Assignment"

Wireless Coverage

An Access Point establishes an average communication range with MUs called a *Basic Service Set (BSS)* or cell. When in a particular cell, the MU associates and communicates with the Access Point supporting the radio coverage area of that cell. Adding Access Points to a single LAN establishes more cells to extend the range of the network. Configuring the same *ESSID (Extended Service Set Identifier)* on all Access Points makes them part of the same Wireless LAN.

Access points with the same ESSID define a coverage area. A valid ESSID is an alphanumeric, case-sensitive identifier up to 32 characters. An MU searches for an Access Point with a matching ESSID and synchronizes (associates) to establish communications. This device association allows MUs within the coverage area to move about or *roam.* As the MU roams from cell to cell, it associates with a different Access Point. The roam occurs when the MU analyzes the reception quality at a location and determines a different provides better signal strength and lower MU load distribution.

If the MU does not find an Access Point with a workable signal, it can perform a scan to find any AP. As MUs controller APs, the AP updates its association statistics.

The user can configure the ESSID to correspond to up to 16 WLANs on each 802.11a/n or 802.11b/g/n radio. A *Wireless Local Area Network (WLAN)* is a data-communications system that flexibly extends the functionalities of a wired LAN. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable. Within the WLAN, roaming users can be handed off from one Access Point to another like a phone system. WLANs can therefore be configured around the needs of specific groups of users, even when they are not in physical proximity.

MAC Layer Bridging

The Access Point provides *MAC layer bridging* between its interfaces. The Access Point monitors traffic from its interfaces and, based on frame address, forwards the frames to the proper destination. The Access Point tracks source and destination addresses to provide intelligent bridging as MUs roam or network topologies change. The Access Point also handles broadcast and multicast messages and responds to MU association requests.

The Access Point listens to all packets on its LAN and WAN interfaces and builds an address database using MAC addresses. An address in the database includes the interface media that the device uses to associate with the Access Point. The Access Point uses the database to forward packets from one interface to another. The bridge forwards packets addressed to unknown systems to the *Default Interface* (Ethernet).

The Access Point internal stack interface handles all messages directed to the Access Point. Each stores information on destinations and their interfaces to facilitate *forwarding*. When a user sends an *ARP (Address Resolution Protocol)* request packet, the Access Point forwards it over all enabled interfaces except over the interface the ARP request packet was received.

On receiving the ARP response packet, the Access Point database keeps a record of the destination address along with the receiving interface. With this information, the Access Point forwards any directed packet to the correct destination. Transmitted ARP request packets echo back to other MUs. The Access Point removes from its database the destination or interface information not used for a specified time. The AP refreshes its database when it transmits or receives data from these destinations and interfaces.

Media Types

The Access Point radio interface conforms to IEEE 802.11 specifications. The Access Point supports multiple-cell operations with fast roaming between cells. Within a direct-sequence system, each cell can operate independently. Adding cells to the network provides an increased coverage area and total system capacity.

The serial port provides a *Command Line Interface (CLI)* connection. The serial link supports a direct serial connection. The Access Point is a *Data Terminal Equipment (DTE)* device with male pin connectors for the RS-232 port. Connecting the Access Point to a PC requires a null modem serial cable.

Direct-Sequence Spread Spectrum

Spread spectrum (broadband) uses a narrowband signal to spread the transmission over a segment of the radio frequency band or spectrum. Direct-sequence is a spread spectrum technique where the transmitted signal is spread over a particular frequency range. The Access Point uses *Direct-Sequence Spread Spectrum (DSSS)* for radio communication.

Direct-sequence systems communicate by continuously transmitting a redundant pattern of bits called a *chipping sequence.* Each bit of transmitted data is mapped into chips by the Access Point and rearranged into a pseudorandom spreading code to form the chipping sequence. The chipping sequence is combined with a transmitted data stream to produce the output signal.

MUs receiving a direct-sequence transmission use the spreading code to map the chips within the chipping sequence back into bits to recreate the original data transmitted by the Access Point. Intercepting and decoding a direct-sequence transmission requires a predefined algorithm to associate the spreading code used by the transmitting Access Point to the receiving MU. This algorithm is established by IEEE 802.11b specifications. The bit redundancy within the chipping sequence enables the receiving MU to recreate the original data pattern, even if bits in the chipping sequence are corrupted by interference.

The ratio of chips per bit is called the *spreading ratio*. A high spreading ratio increases the resistance of the signal to interference. A low spreading ratio increases the bandwidth available to the user. The Access Point uses different modulation schemes to encode more bits per chip at higher data rates.

MU Association Process

An Access Point recognizes MUs as they begin the association process. An Access Point keeps a list of the MUs it services. MUs associate with an Access Point based on the following conditions:

- Signal strength between the Access Point and the MU
- Number of MUs currently associated with the Access Point
- MUs encryption and authentication capabilities
- MUs supported data rate

MUs perform pre-emptive roaming by intermittently scanning for Access Points and associating with the best available Access Point. Before roaming and associating, MUs perform full or partial scans to collect statistics and determine the direct-sequence channel used by the Access Point.

Scanning is a periodic process where the MU sends out probe messages on all channels defined by the country code. The statistics enable an MU to reassociate by synchronizing its channel to the Access Point. The MU continues communicating with that Access Point until it needs to switch cells or roam.

MUs perform partial scans at programmed intervals, when missing expected beacons or after excessive transmission retries. In a partial scan, the MU scans Access Points classified as proximate on the Access Point table. For each channel, the MU tests for *Clear Channel Assessment* (CCA). The MU broadcasts a probe with the ESSID and broadcast BSS_ID when the channel is transmission-free. It sends an ACK to a directed probe response from the Access Point and updates the table.

An MU can roam within a coverage area by switching Access Points. Roaming occurs when:

- Unassociated MU attempts to associate or reassociate with an available Access Point
- Supported rate changes or the MU finds a better transmit rate with another Access Point
- *RSSI (received signal strength indicator)* of a potential Access Point exceeds the current Access Point
- Ratio of good-transmitted packets to attempted-transmitted packets that fall below a threshold.

An MU selects the best available Access Point and adjusts itself to the Access Point direct-sequence channel to begin association. Once associated, the Access Point begins forwarding frames addressed to the target MU. Each frame contains fields for the current direct-sequence channel. The MU uses these fields to resynchronize to the Access Point.

The scanning and association process continues for active MUs. This process allows MUs to find new Access Points and discard out-of-range or deactivated Access Points. By testing the airwaves, MUs can choose the best network connection available.

Operating Modes

The Access Point can operate in a couple of configurations.

- *Access Point*—As an *Access Point*, the Access Point functions as a layer 2 bridge. The wired uplink can operate as a trunk and support multiple VLANs. Up to 16 WLANs can be defined and mapped to Access Point WLANs. Each WLAN can be configured to be broadcast by one or both Access Point radios. An Altitude 4710 or Altitude 4750 can operate in both an Access Point mode and Wireless Gateway/Router mode simultaneously. The network architecture and Access Point configuration define how the Access Point and Wireless Gateway/Router mode are negotiated.
- *Wireless Gateway/Router*—If operating as a *Wireless Gateway/Router*, the Access Point functions as a router between two layer 2 networks: the WAN uplink (the ethernet port) and the Wireless side. The following options are available providing a solution for single-cell deployment:
- *PPPoE*—The WAN interface can terminate a PPPoE connection, thus enabling the Access Point to operate in conjunction with a DSL or Cable modem to provide WAN connectivity.
- *NAT—(Network Address Translation)* on the Wireless interface. Using NAT, the router is able to manage a private IP scheme. NAT allows translation of private addresses to the WAN IP address.
- *DHCP*—The Access Point can assign private IP addresses.
- *Firewall*—A Firewall protects against a number of known attacks.

Management Access Options

Managing the Access Point includes viewing network statistics and setting configuration options. Statistics track the network activity of associated MUs and data transfers on the AP interfaces.

The Access Point requires one of the following connection methods to perform a custom installation and manage the network:

- *Secure Java-Based WEB UI*—(use *Sun Microsystems' JRE 1.5* or higher available from Sun's Web site and be sure to disable Microsoft's Java Virtual Machine if installed)
- *Command Line Interface (CLI)* via Serial, Telnet and SSH
- *Config file*—Human-readable; Importable/Exportable via FTP and TFTP
- *MIB (Management Information Base)* accessing the Access Point SNMP function using a MIB Browser. The Access Point's download site contains the following MIB files supporting the Access Point:
  - EXTR-CC-AP4700-MIB-2.0 (standard MIB file)
  - EXTR-AP4700-MIB-02a02

Make configuration changes to Access Point's individually. Optionally, use the Access Point import/export configuration function to download settings to other Access Points.

For detailed information, see "Importing/Exporting Configurations" on page 114.

MAC Address Assignment

MAC address assignments are as follows:

- *LAN (GE1)*—The Access Point MAC address can be found underneath the Access Point chassis.
- *WAN (GE2)*—The number of the LAN MAC address + 1.
- *LAN2*—A virtual LAN not mapped to the LAN Ethernet port. This address is the lowest of the two radio MAC addresses.

- *Radio1 (802.11b/g/n)*—Random address located on the Web UI, CLI and SNMP interfaces.
- *Radio2 (802.11a/n)*—Random address located on the Web UI, CLI and SNMP interfaces.

The Access Point’s BSS (virtual AP) MAC addresses are calculated as follows:

- *BSS1*—The same as the corresponding base radio’s MAC address.
- *BSS2*—Base radio MAC address +1
- *BSS3*—Base radio MAC address +2
- *BSS4*—Base radio MAC address +3

2 CHAPTER Hardware Installation

An Altitude 4700 Series Access Point installation includes mounting the Access Point, connecting the Access Point to the network, connecting antennae and applying power. Installation procedures vary for different environments. See the following sections for more details:

- Precautions on page 45
- Requirements on page 45
- Package Contents on page 46
- Access Point Placement on page 47
- Power Options on page 48
- Power Injector System on page 48
- Mounting an Altitude 4700 Series Access Point on page 50
- LED Indicators on page 57
- Setting Up MUs on page 60

CAUTION

Extreme Networks recommends conducting a radio site survey prior to installing an Access Point. A site survey is an excellent method of documenting areas of radio interference and providing a tool for device placement.

Precautions

Before installing an Altitude 4700 Series Access Point, verify the following:

- Do not install in wet or dusty areas without additional protection. Contact an Extreme Networks representative for more information.
- Verify the environment has a continuous temperature range between -20° C to 50° C.

Requirements

The minimum installation requirements for a single-cell, peer-to-peer network:

- An Altitude 4700 Series Access Point

- 48 Volt Power Supply
- A power outlet
- Dual-band antennae or an antenna specifically supporting the AP’s 2.4 or 5 GHz band

Package Contents

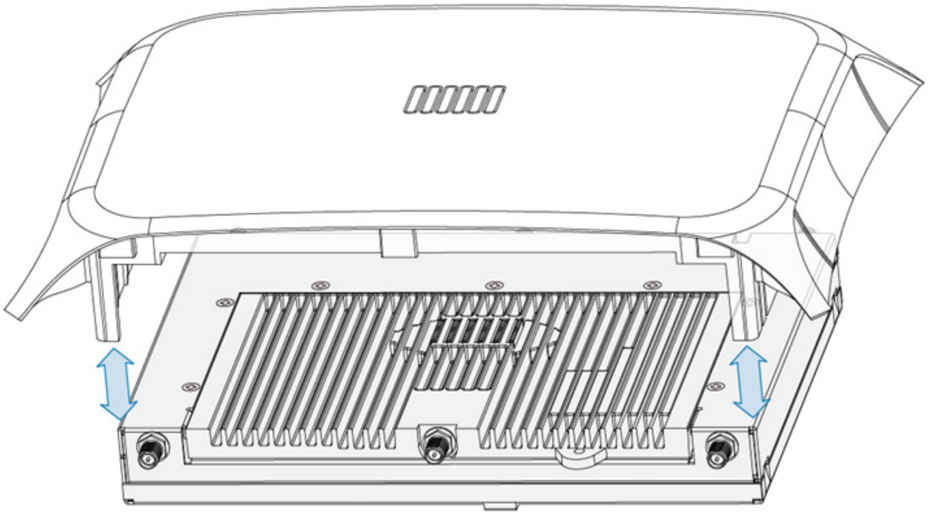
Check package contents for the correct model and accessories. Each available configuration (at a minimum), contains:

- Altitude 4700 Series Access Point (accessories dependent on SKU ordered)
- Altitude 4700 Series Access Point Installation Guide (supports both Altitude 4710 and Altitude 4750 models)
- China ROHS compliance addendum
- Wall mount screw and anchor kit
- Accessories Bag (4 rubber feet and an LED light pipe and badge with label for above the ceiling installations)

Contact the Extreme Networks Support Center to report missing or improperly functioning items.

NOTE

The Access Point façade with 6 Element Antenna is separately orderable and provides an integrated antenna option. The facade connects to the Access Point as illustrated. Once attached, the LEDs continue to illuminate through the facade. Contact your Extreme Networks sales associate for information on ordering a facade with your Access Point.



Access Point Placement

For optimal performance, install the Access Point away from transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators and other industrial equipment. Signal loss can occur when metal, concrete, walls or floors block transmission. Install the Access Point in an open area or add Access Points as needed to improve coverage.

Antenna coverage is analogous to lighting. Users might find an area lit from far away to be not bright enough. An area lit sharply might minimize coverage and create *dark areas.* Uniform antenna placement in an area (like even placement of a light bulb) provides even, efficient coverage.

Place the Access Point using the following guidelines:

- Install the Access Point at an ideal height of 10 feet from the ground.
- Orient the Access Point antennas vertically for best reception.
- Point the Access Point antennas downward if attaching to the ceiling.

To maximize the Access Point's radio coverage area, Extreme Networks recommends conducting a site survey to define and document radio interference obstacles before installing the Access Point.

Site Surveys

A site survey analyzes the installation environment and provides users with recommendations for equipment and placement. The optimum placement of 802.11a/n Access Points differs from 802.11b/g/n Access Points, because the locations and number of Access Points required are different to support the radio coverage area.

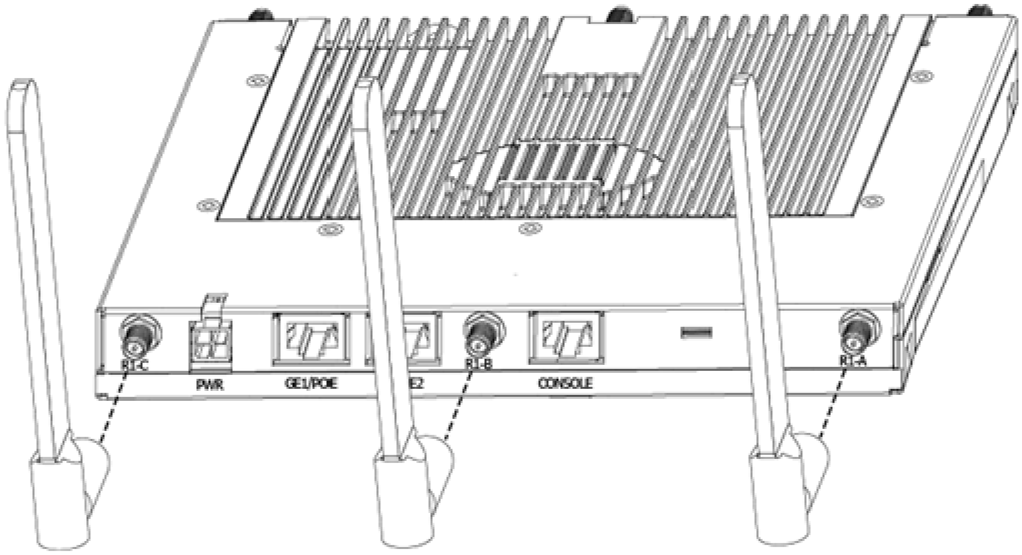
Extreme Networks recommends conducting a new site survey and developing a new coverage area floor plan when switching from legacy Access Points (Altitude 3500 models) to a new Altitude 4700 series model, as the device placement requirements *could be* significantly different.

Antenna Options

Extreme Networks supports two antenna suites for Altitude 4700 series models. One antenna suite supporting the 2.4 GHz band and another antenna suite supporting the 5 GHz band. Select an antenna model best suited to the intended operational environment of your Access Point. If a three radio Altitude 4750 is purchased, the Access Point ships with a single antenna connected to the Access Point chassis (next to the existing R1-A connector). This antenna is in addition to the other six antennas available to the Access Point's other two radios. The single antenna supporting the Altitude 4750 Access Point's third radio supports sensor mode only and can not function as a WLAN radio.

NOTE

On a dual-radio model, Radio 1 refers to the 2.4 GHz radio and Radio 2 refers to the 5 GHz radio. However, there could be some cases where a dual-radio Access Point is performing a Rogue AP detector function. In this scenario, the Access Point is receiving in either 2.4 GHz or 5 GHz over the Radio 1 or Radio 2 antennae depending on which radio is selected for the scan.



R1 defines the Access Point’s radio 1 antenna connectors and R2 defines radio 2 antenna connectors.

The supported 2.4 GHz antenna suite and 5 GHz antenna suite are given in the *Altitude 35xx/46xx/47xx AP Antenna Selection Guide, Rev.xx*.

Power Options

The power options for an Altitude 4700 Series Access Point include:

- 48-Volt Power Supply
- Power Injector (Part No. AP-PSBIAS-1P3-AFR)

CAUTION

A single-port Gigabit Power-over-Ethernet Power Injector (Part No. AP-PSBIAS-1P3-AFR) is available for use with the AP4700 access point.

Power Injector System

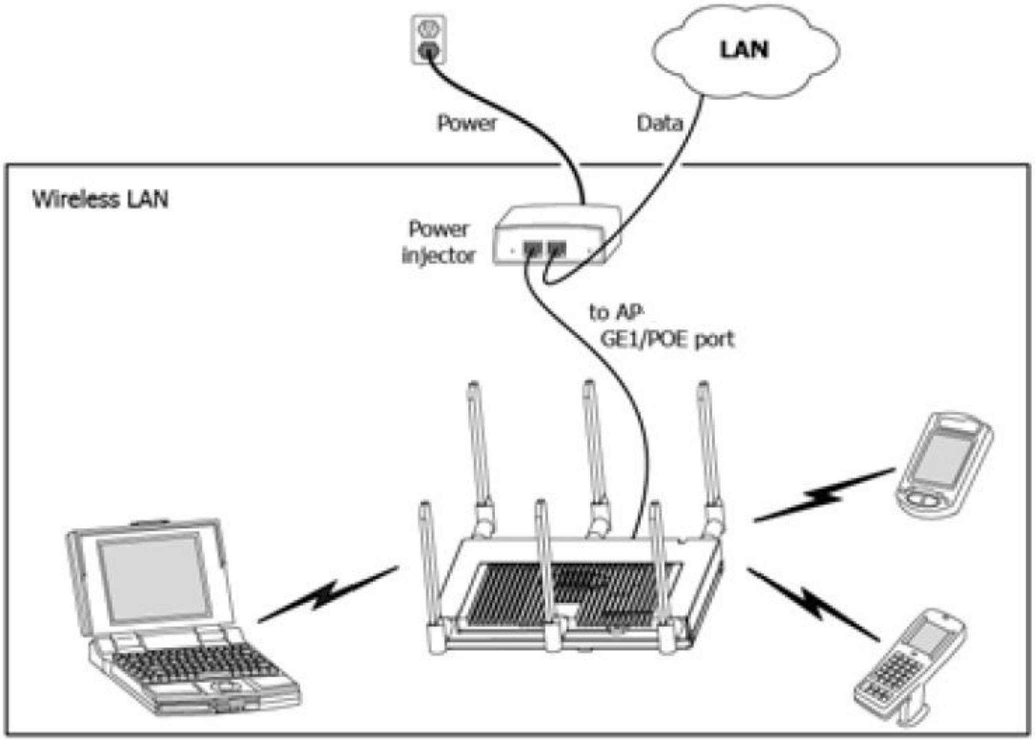
The AP4700 access point can receive power via an Ethernet cable connected to the access point’s GE1/POE (LAN) port.

When users purchase a WLAN solution, they often need to place access points in obscure locations. In the past, a dedicated power source was required for each access point in addition to the Ethernet infrastructure. This often required an electrical contractor to install power drops at each access point location. The Power Injector merges power and Ethernet into one cable, reducing the burden of installation and allowing optimal access point placement in respect to the intended coverage area.

The Power Injector (Part No. AP-PSBIAS-1P3-AFR) is a high power Gigabit POE Injector delivering up to 30 watts. The access point can only use a Power Injector when connecting the unit to the access point's GE1/POE port. The Power Injector is a separately ordered component and not shipped with an existing access point SKU.

An AP4700 access point can also be used with the 3af power injector (AP-PSBIAS-1P2-AFR). However, AP functionality is limited when powered by an AP-PSBIAS-1P2-AFR, since the AP has Ethernet connectivity limited to only the GE1 port.

Extreme Networks is reselling Motorola Power Supply (Part No. 50-14000-247R) as an accessory for AP4700.



CAUTION

The access point supports any standards-based compliant POE sources (802.3at and 802.3af). Using a non-standard based solution could either limit functionality or severely damage the access point and void the product warranty.

A separate Power Injector is required for each access point comprising the network.

Installing the Power Injector

Refer to the following sections for information on planning, installing, and validating the installation:

- Preparing for Site Installation on page 50
- Cabling the Power Injector on page 50

Preparing for Site Installation

The Power Injector can be installed free standing on an even horizontal surface or wall mounted using the unit's wall mounting key holes. The following guidelines should be adhered to before cabling the Power Injector to an Ethernet source and access point:

- Do not block or cover airflow to the Power Injector.
- Keep the unit away from excessive heat, humidity, vibration and dust.
- The Power Injector is not a repeater, and does not amplify the Ethernet data signal. For optimal performance, ensure the unit is placed as close as possible to the network data port.

CAUTION

To avoid problematic performance and restarts, disable POE from a wired switch port connected to an access point if mid-span power sourcing equipment (PSE) is used between the two, regardless of the manufacturer of the switch.

Cabling the Power Injector

To install a Power Injector to an Ethernet data source and an access point:

CAUTION

Ensure AC power is supplied to the Power Injector using an AC cable with an appropriate ground connection approved for the country of operation.

1 Connect an RJ-45 Ethernet cable between the network data supply (host) and the Power Injector's Data In connector.

2 Connect an RJ-45 Ethernet cable between the Power Injector's Data & Power Out connector and the access point's GE1/POE port.

CAUTION

Cabling a Power Injector to the WAN port (GE2) renders the AP nonoperational. Only use an AP-PSBIAS-1P3-AFR (or AP-PSBIAS-1P2-AFR at worse access point performance) Power Injector with the access point's GE1/POE (LAN) port.

Ensure the cable length from the Ethernet source (host) to the Power Injector and access point does not exceed 100 meters (333 ft). The Power Injector has no On/Off power switch.

The Power Injector receives power and is ready for access point connection and operation as soon as AC power is applied. Refer to the Installation Guide shipped with the Power Injector for a description of the device's LED behavior.

3 Verify all cable connections are complete before supplying power to the access point.

Mounting an Altitude 4700 Series Access Point

The Altitude 4700 Series Access Point can attach to a wall, mount under a suspended T-Bar or above a ceiling (plenum or attic) following the same installation instructions. Choose one of the following mounting options based on the physical environment of the coverage area. Do not mount the Access Point in a location that has not been approved in a site survey.

Refer to the following, depending on how you intend to mount the Access Point:

- Wall Mounted Installations on page 51
- Suspended Ceiling T-Bar Installations on page 53
- Above the Ceiling (Plenum) Installations on page 55

Wall Mounted Installations

Wall mounting requires hanging the Access Point along its width (or length) using the pair of slots on the bottom of the unit and using the Access Point mounting template for the screws.

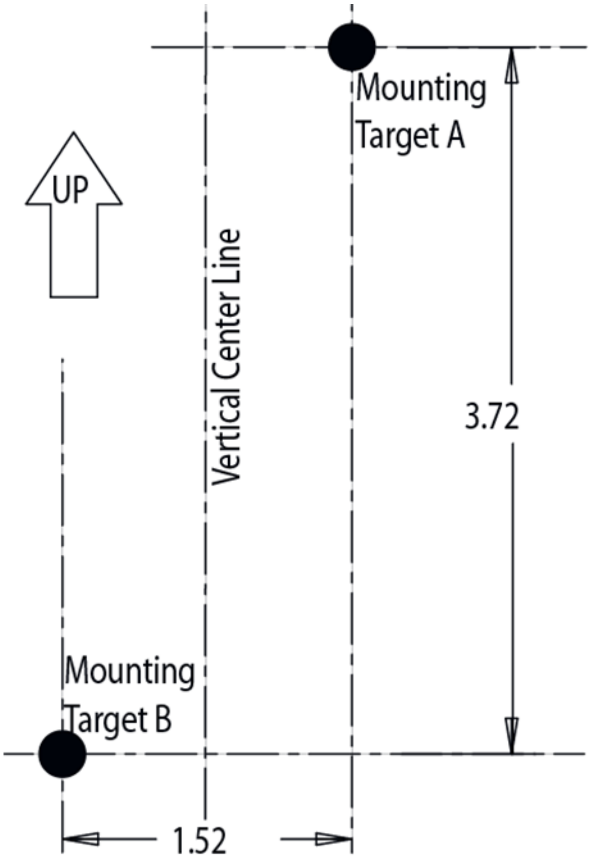
CAUTION

An Access Point should be wall mounted to concrete or plaster-wall-board (dry wall) only. Do not wall mount an Access Point to combustible surfaces.

The hardware and tools (customer provided) required to install the Access Point on a wall consists of:

- Two Phillips pan head self-tapping screws (ANSI Standard) #6-18 X 0.875in. Type A or AB Self-Tapping screw, or (ANSI Standard Metric) M3.5 X 0.6 X 20mm Type D Self-Tapping screw
- Two wall anchors
- Wall mount template
- Security cable (optional third part provided accessory)

To mount the Access Point on a wall use the following template:



1 Photocopy the template (on the previous page) to a blank piece of paper. Do not reduce or enlarge the scale of the template.

CAUTION

If printing the mounting template (on the previous page) from an electronic PDF, dimensionally confirm the template by measuring each value for accuracy.

2 Tape the template to the wall mounting surface.
- If the installation requires the antenna be positioned vertically, the centerline reference (of the template) needs to be positioned vertically. The cabling shall exit the Access Point in a vertical direction.
- If the installation requires the antenna be positioned horizontally, the vertical centerline (of the template) needs to be positioned horizontally. The cabling shall exit the Access Point in a horizontal direction.

3 At mounting targets A and B, mark the mounting surface through the template at the target center.

4 Discard the mounting template.

5 At each point, drill a hole in the wall, insert an anchor, screw into the anchor the wall mounting screw and stop when there is 1mm between the screw head and the wall.

If pre-drilling a hole, the recommended hole size is 2.8mm (0.11in.) if the screws are going directly into the wall and 6mm (0.23in.) if wall anchors are being used.

6 If required, install and attach a security cable to the Access Point's lock port.

7 Attach the antennas to their correct connectors.

For more information on available antennas, see "Antenna Options" on page 47.

8 Place the large center opening of each of the mount slots over the screw heads.

9 Slide the Access Point down along the mounting surface to hang the mount slots on the screw heads.

CAUTION

Ensure you are placing the antennas on the correct connectors to ensure the successful operation of the Access Point.

NOTE

It is recommended the Access Point be mounted with the RJ45 cable connector oriented upwards or downwards to ensure proper operation.

10 Cable the Access Point using an approved line cord and power supply.

For standard 48-Volt Power Adapter and line cord installations:

a Connect an RJ-45 CAT5e (or CAT6) Ethernet cable between the network data supply (host) and the Access Point's GE1/POE port.

b Verify the power adapter is correctly rated according the country of operation.

c Connect the power supply line cord to the power adapter.

d Attach the power adapter cable into the power connector on the Access Point.

e Plug the power adapter into an outlet.

11 Verify the behavior of the Access Point's LEDs. For more information, see "LED Indicators" on page 57.

The Access Point is ready to configure. For information on an Access Point default configuration, see "Getting Started" on page 63. For specific details on system configurations, see "System Configuration" on page 77.

Suspended Ceiling T-Bar Installations

A suspended ceiling mount requires holding the Access Point up against the T-bar of a suspended ceiling grid, and twisting the chassis onto the T-bar.

The mounting tools (customer provided) and hardware required to install the Access Point on a ceiling T-bar consists of:

- Safety wire (recommended and customer supplied)
- Security cable (and customer supplied)

To install the Access Point on a ceiling T-bar:

1 Extreme Networks recommends you loop a safety wire—with a diameter of at least 1.01 mm (.04 in.), but no more than 0.158 mm (.0625 in.)—through the tie post (above the console connector) and secure the loop.

2 If desired, install and attach a security cable to the Access Point's lock port.

3 Attach the radio antennas to their correct connectors.

For more information on available antennas, see "Antenna Options" on page 47.

4 Cable the Access Point using the approved power supply.

CAUTION

Do not supply power to the Access Point until the cabling of the unit is complete.

a Connect an RJ-45 CAT5e (or CAT6) Ethernet cable between the network data supply (host) and the Access Point's GE1/POE port.

b Verify the power adapter is correctly rated according the country of operation.

c Ensure the cable length from the Ethernet source to the Power Injector and access point does not exceed 100 meters (333 ft). The Power Injector has no On/Off power switch. The Power Injector receives power as soon as AC power is applied. For more information on using the Power Injector, see "Power Injector System" on page 48.

5 Verify the behavior of the LEDs. For more information, see "LED Indicators" on page 57.

6 Align the bottom of the ceiling T-bar with the back of the Access Point.

7 Orient the Access Point's chassis by its length and the length of the ceiling T-bar.

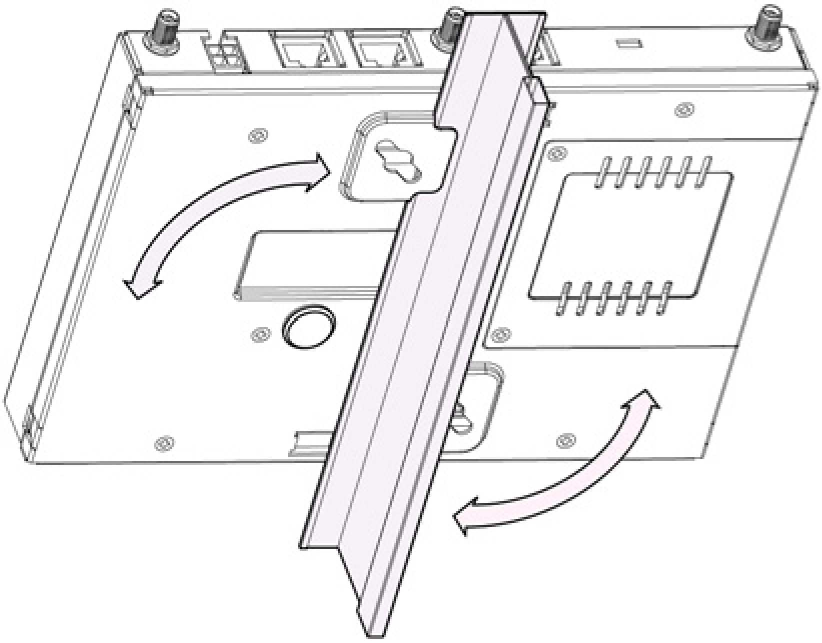
8 Rotate the Access Point chassis 45 degrees clockwise.

9 Push the back of the Access Point chassis on to the bottom of the ceiling T-bar.

CAUTION

Ensure the safety wire and cabling used in the T-Bar installation is securely fastened to the building structure in order to provide a safe operating environment.

10 Rotate the Access Point chassis 45 degrees counter-clockwise. The clips click as they fasten to the T-bar.



11 The Access Point is ready to configure. For information on an Access Point default configuration, see "Getting Started" on page 63. For specific details on Access Point system configurations, see "System Configuration" on page 77.

Above the Ceiling (Plenum) Installations

An above the ceiling installation requires placing the Access Point above a suspended ceiling and installing the provided light pipe under the ceiling tile for viewing the rear panel status LEDs of the unit. An above the ceiling installation enables installations compliant with drop ceilings, suspended ceilings and industry standard tiles from .625 to .75 inches thick.

NOTE

The Altitude 4700 Series Access Points are Plenum rated to UL2043 and NEC1999 to support above the ceiling installations.

CAUTION

Extreme Networks does not recommend mounting the Access Point directly to any suspended ceiling tile with a thickness less than 12.7mm (0.5in.) or a suspended ceiling tile with an unsupported span greater than 660mm (26in.). Extreme Networks strongly recommends fitting the Access Point with a safety wire suitable for supporting the weight of the device. The safety wire should be a standard ceiling suspension cable or equivalent steel wire between 1.59mm (.062in.) and 2.5mm (.10in.) in diameter.

The mounting hardware required to install the Access Point above a ceiling consists of:

- Light pipe
- Badge for light pipe
- Decal for badge

- Safety wire (strongly recommended)
- Security cable (optional)

To install the Access Point above a ceiling:

1 If possible, remove the adjacent ceiling tile from its frame and place it aside.

2 Install a safety wire, between 1.5mm (.06in.) and 2.5mm (.10in.) in diameter, in the ceiling space.

3 If required, install and attach a security cable to the Access Point's lock port.

4 Mark a point on the finished side of the tile where the light pipe is to be located.

5 Create a light pipe path hole in the target position on the ceiling tile.

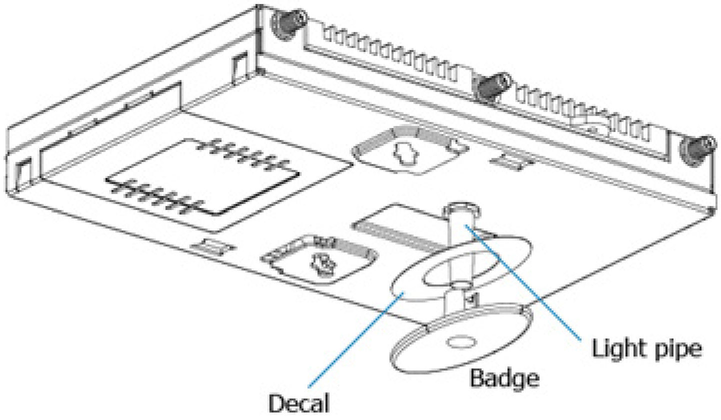
6 Use a drill to make a hole in the tile the approximate size of the LED light pipe.

CAUTION

Extreme Networks recommends care be taken not to damage the finished surface of the ceiling tile when creating the light pipe hole and installing the light pipe.

7 Remove the light pipe's rubber stopper before installing the light pipe.

8 Connect the light pipe to the bottom of the Access Point. Align the tabs and rotate approximately 90 degrees. Do not over tighten.



9 Fit the light pipe into hole in the tile from its unfinished side.

10 Place the decal on the back of the badge and slide the badge onto the light pipe from the finished side of the tile.

11 Attach the radio antennas to their correct connectors. For more information on available antennas, see "Antenna Options" on page 47.

12 Extreme Networks recommends attaching safety wire to the Access Point's safety wire tie point or security cable (if used) to the Access Point's lock port.

13 Align the ceiling tile into its former ceiling space.

14 Cable the Access Point using an approved line cord and power supply.

CAUTION

Do not supply power to the Access Point until the cabling of the unit is complete.

- **a** Connect an RJ-45 CAT5e (or CAT6) Ethernet cable between the network data supply (host) and the Access Point's GE1/POE port.
- **b** Verify the power adapter is correctly rated according the country of operation.
- **c** Ensure the cable length from the Ethernet source to the Power Injector and access point does not exceed 100 meters (333 ft). The Power Injector has no On/Off power switch The Power Injector receives power as soon as AC power is applied. For more information on using the Power Injector, see "Power Injector System" on page 48.

15 Verify the behavior of the LEDs. For more information, see "LED Indicators" on page 57.

16 Place the ceiling tile back in its frame and verify it is secure.

The Access Point is ready to configure. For information on an Access Point default configuration, see "Getting Started" on page 63. For specific details on system configurations, see "System Configuration" on page 77.

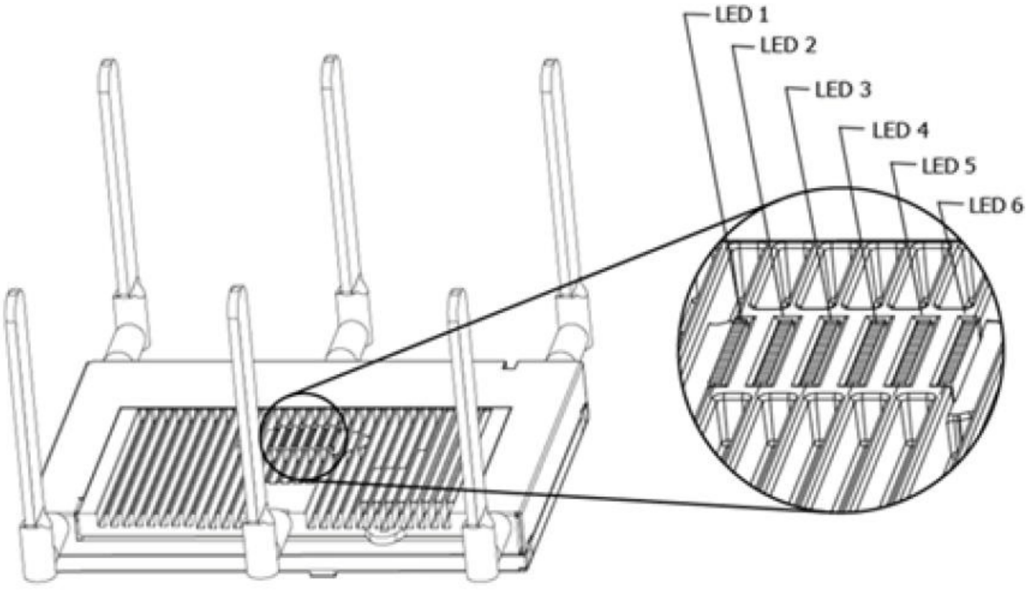
LED Indicators

Altitude 4700 Series Access Points have six LEDs on the top of the Access Point housing, and one optional LED light pipe at the bottom of the unit. However, an Altitude 4710 model Access Point does not use LED 6, as no third radio is available. Five LEDs illuminate (on top of the housing) for dual radio models.

The Access Point utilizes two (different colored) lights below each LED. Only one light displays within an LED at any given time. Every light within each LED is exercised during startup to allow the user to see if an LED is non-functional. The LEDs turn on and off while rotating around in a circle. Since two LEDs feed each light pipe, the pattern is from left to right, then right to left.

NOTE

LED blink rate is proportional to activity. The busiest traffic corresponds to the fastest blink, while the slowest traffic corresponds to slowest blink.



NOTE

Depending on how the 5 GHz and 2.4 GHz radios are configured, the LEDs will blink at different intervals between amber and yellow (5 GHz radio) and emerald and yellow (2.4 GHz radio).

The LEDs on the top housing of the Access Point are clearly visible in wall and below ceiling installations. The top housing LEDs have the following display and functionality.

Three Radio Altitude 4750 LEDs

A three radio model Altitude 4750 has the following unique LED behavior:

LED 1	LED 2 (LAN)	LED 3 (WAN)	LED 4 - 5 GHz	LED 5 - 2.4 GHz	LED 6

Blinking **Red** indicates booting. Solid **Red** defines the diagnostic mode. **White** defines normal operation.	**Green** defines normal GE1 operation.	**Green** defines normal GE2 operation.	Blinking **Amber** indicates 802.11a activity. A 5 second **Amber** and **Yellow** blink rate defines 802.11an activity. A 2 second **Amber** and **Yellow** blink rate defines 802.11an (40 MHz) activity. When functioning as a sensor, LED alternates between **Amber** and **Yellow**. The blink interval is 0.5 seconds. It's 1 second when no Server is connected.	Blinking **Emerald** indicates 802.11bg activity. A 5 second **Emerald** and **Yellow** blink rate defines 802.11bgn activity. A 2 second **Emerald** and **Yellow** blink rate defines 802.11bgn (40 MHz) activity. When functioning as a sensor, LED alternates between **Emerald** and **Yellow**. The blink interval is 0.5 seconds. It's 1 second when no Server is connected.	Blinking **Emerald** indicates the radio is defined as a sensor, but is disabled. Alternates between **Emerald** and **Amber** when the radio is defined as a sensor with no Server connected. The blink interval is 1 second. Alternates between **Emerald** and **Amber** when the radio is defined as a sensor and a Server is connected. The blink interval is 0.5 seconds.

Dual Radio (2.4/5 GHz) LEDs

A dual radio (2.4/5 GHz) model Access Point has the following unique LED behavior:

LED 1	LED 2 (LAN)	LED 3 (WAN)	LED 4 - 5 GHz	LED 5 - 2.4 GHz	LED 6
Blinking **Red** indicates booting.Solid **Red** defines the diagnostic mode. **White** defines normal operation.	**Green** defines normal GE1 operation.	**Green** defines normal GE2 operation.	Blinking **Amber** indicates 802.11a activity. A 5 second **Amber** and **Yellow** blink rate defines 802.11an activity. A 2 second **Amber** and **Yellow** blink rate defines 802.11an (40 MHz) activity. When functioning as a sensor, LED alternates between **Amber** and **Yellow**. The blink interval is 0.5 seconds. It's 1 second when no Server is connected.	Blinking **Emerald** indicates 802.11bg activity. A 5 second **Emerald** and **Yellow** blink rate defines 802.11bgn activity. A 2 second **Emerald** and **Yellow** blink rate defines 802.11bgn (40 MHz) activity. When functioning as a sensor, LED alternates between **Emerald** and **Yellow**. The blink interval is 0.5 seconds. It's 1 second when no Server is connected.	Not used

Rear LED

The LED on the rear (bottom) of the Access Point is optionally viewed using a single (customer installed) extended light pipe, adjusted as required to suit above the ceiling installations. The LED light pipe has the following color display and functionality:

LED 7
Blinking **Red** (160 msec) indicates a failure condition.
Solid **Red** defines the diagnostic mode.
White defines normal operation.

Setting Up MUs

Legacy MUs

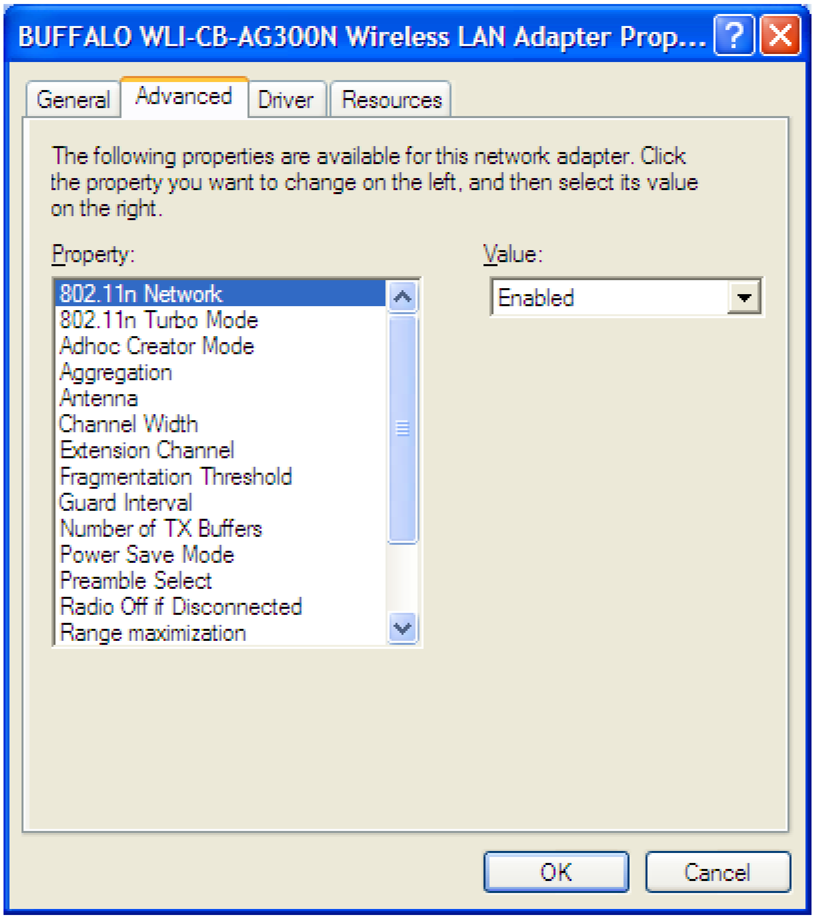
For a discussion of how to initially test the access point to ensure it can interoperate with the MUs intended for its operational environment, see "Basic Device Configuration" on page 65 and specifically "Testing Connectivity" on page 74.

802.11n MUs

Third-party 802.11n clients can connect to the Access Point using default settings with no additional user intervention. However, there could be instances where the specific (high-performance) 802.11n settings cannot be sustained due to adverse radio traffic conditions within the network. When this occurs, Extreme Networks recommends changing the Windows XP settings so the adapter can use settings defined for legacy (802.11a/bg) adapter operation. Once network conditions improve, use Windows XP to re-enable the adapter for 802.11n support.

To change the Access Point's settings to support legacy 802.11a/bg operation (using Windows XP):

1. Select *My Network Places.*
2. Right-click and select *Properties.* The *Network Connections* screen displays.
3. Select (right-click on) the adapter supporting 802.11n operation with the Access Point and select *Properties*.
4. Click on the *Configure* button.
5. The Network Connection screen displays supporting the 802.11n adapter.
6. Select the *Advanced* tab.
7. Select *802.11n Network* from the Property field and select either *Enable* or *Disable* from the Value drop-down menu.
8. Select *Disable* when the 802.11n rate settings and performance values defined on the Access Point cannot be sustained (due to network congestion or interference). Once network conditions improve to the point where 802.11n traffic can be sustained, enable the *802.11n Network* parameter once again.



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- 802.11n Network
- 802.11n Turbo Mode
- Adhoc Creator Mode
- Aggregation
- Antenna
- Channel Width
- Extension Channel
- Fragmentation Threshold
- Guard Interval
- Number of TX Buffers
- Power Save Mode
- Preamble Select
- Radio Off if Disconnected
- Range maximization

Value: Enabled

NOTE

If re-enabling the adapter for 802.11 support, ensure additional 802.11n settings (Aggregation, Channel Width, Guard Interval etc.) are also enabled to ensure optimal operation.

9 Click *OK* to save the updates to the adapter's configuration.

3
CHAPTER

Getting Started

The Access Point should be installed in an area tested for radio coverage using one of the site survey tools available to the field service technician. Once an installation site has been identified, the installer should carefully follow the hardware precautions, requirements, mounting guidelines and power options outlined in "Hardware Installation" on page 45.

See the following sections for more details:

- Installing the Access Point on page 63
- Configuration Options on page 64
- Basic Device Configuration on page 65

Installing the Access Point

Make the required cable and power connections before mounting the Access Point in its final operating position. Test the Access Point with an associated MU before mounting and securing the Access Point. Carefully follow the mounting instructions in one of the following sections to ensure the Access Point is installed correctly:

- For instructions on mounting the Access Point to a wall, see "Wall Mounted Installations" on page 51.
- For instructions on mounting an Access Point to a ceiling T-bar, see "Suspended Ceiling T-Bar Installations" on page 53.
- For instructions on installing the Access Point in an above the ceiling attic space, see "Above the Ceiling (Plenum) Installations" on page 55.

For information on the antenna suite available to the access point, see "Antenna Options" on page 47. To verify LED behavior once installed, see "LED Indicators" on page 57.

Configuration Options

Once installed and powered, the Access Point can be configured using one of several connection techniques. Managing the access point includes viewing network statistics and setting configuration options. The access point requires one of the following connection methods to manage the network:

- *Secure Java-Based WEB UI* - (use *Sun Microsystems' JRE 1.5* or higher available from Sun's Web site. Disable Microsoft's Java Virtual Machine if installed). For information on using the Web UI to set access point default configuration, see "Basic Device Configuration" on page 65 or chapters 4 through 7 of this guide.
- *Command Line Interface (CLI)* via Serial, Telnet and SSH. The Access Point CLI is accessed through the RS232 port, via Telnet or SSH. The CLI follows the same configuration conventions as the device user interface with a few documented exceptions.
- *Config file* - Readable text file; Importable/Exportable via FTP, TFTP and HTTP. Configuration settings for an Access Point can be downloaded from the current configuration of another Access Point meeting the import/export requirements. For information on importing or exporting configuration files, see "Importing/Exporting Configurations" on page 114.
- *MIB (Management Information Base)* accessing the access point SNMP functions using a MIB Browser. The Access Point download package contains the following 2 MIB files:
    - EXTR-CC-AP4700-MIB-2.0 (standard MIB file)
    - EXTR-AP4700-MIB-02a02

Initially Connecting to the Access Point

NOTE

The procedures described below assume this is the first time you are connecting to an Altitude 4700 Series Access Point.

NOTE

The computer being used should be configured to use the same IP address and subnet mask as the Access Point.

Connecting to the Access Point using the WAN Port

To initially connect to the Access Point using the Access Point's WAN port:

1. Connect AC power to the Access Point, as Power-Over-Ether support is not available on the Access Point's WAN (or GE2) port.
2. Start a browser and enter the Access Point's static IP address (10.1.1.1). The default password is "*admin123*."
3. Refer to "Basic Device Configuration" on page 65 for instructions on the initial (basic) configuration of the Access Point.

Connecting to the Access Point using the LAN Port

To initially connect to the Access Point using the Access Point's LAN port:

1. The LAN (or GE1/POE) port default is set to DHCP. Connect the Access Point's GE1/POE port to a DHCP server. The Access Point will receive its IP address automatically.
2. To view the IP address, connect one end of a null modem serial cable to the Access Point and the other end to the serial port of a computer running HyperTerminal or similar emulation program.
3. Configure the following settings:
   - Baud Rate - 19200
   - Data Bits - 8
   - Stop Bits - 1
   - No Parity
   - No Flow Control
4. Press <ESC> or <Enter> to access the Access Point CLI.
5. Enter the default username of "*admin*" and the default password of "*admin123.*"

   As this is the first time you are logging into the Access Point, you are prompted to enter a new password and set the county code. Refer to "Country Codes" on page 627 for a list of each available countries two digit country code.
6. At the CLI prompt (admin>), type "*summary.*"

   The Access Point's LAN IP address will display.
7. Using a Web browser, use the Access Point's IP address to access the Access Point.
8. Refer to "Basic Device Configuration" on page 65 for instructions on the initial (basic) configuration of the Access Point.

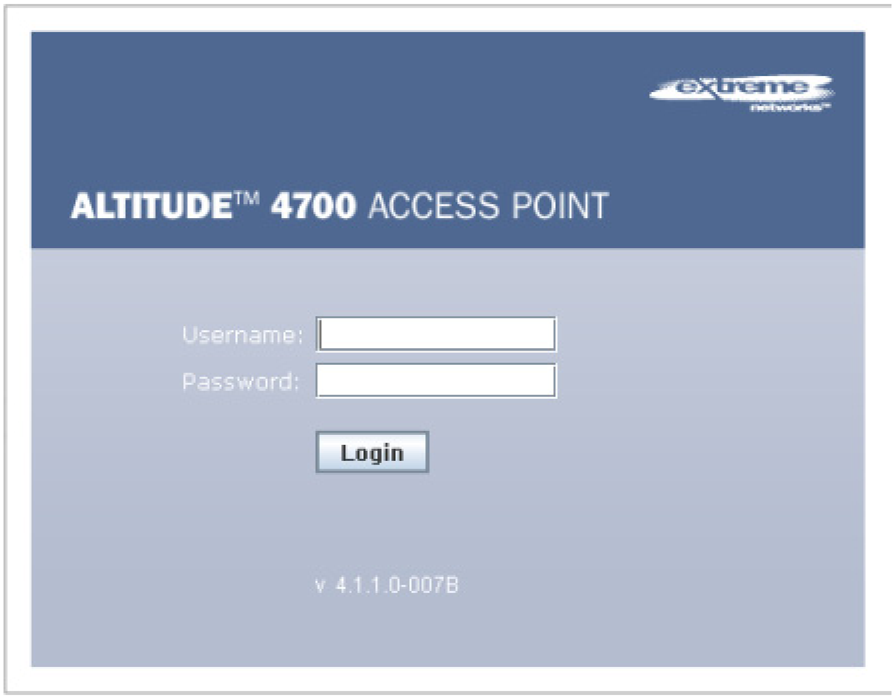
Basic Device Configuration

For the basic setup described in this section, the Java-based Web UI will be used to configure the Access Point. Use the Access Point's LAN interface for establishing a link with the Access Point. Configure the Access Point as a DHCP client. For optimal screen resolution, set your screen resolution to 1024 x 768 pixels or greater.

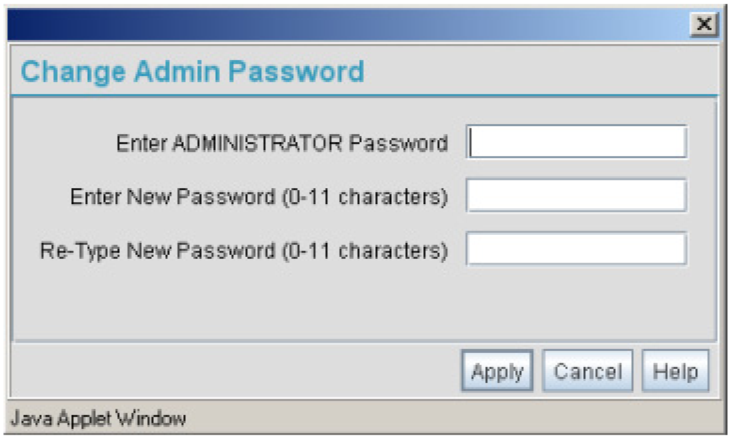
1. Log in using *admin* as the default Username and *admin123* as the default Password. Use your new password if it has been updated from default.

NOTE

For optimum compatibility, use Sun Microsystems JRE 1.5 or higher (available from Sun's website), and be sure to disable Microsoft's Java Virtual Machine if installed.



2 If the default login is successful, the *Change Admin Password* window displays. Change the password.


Change Admin Password
Enter ADMINISTRATOR Password
Enter New Password (0-11 characters)
Re-Type New Password (0-11 characters)
Apply
Cancel
Help
Java Applet Window

Enter the current password and a new admin password in fields provided. Click *Apply*. Once the admin password has been updated, a warning message displays stating the Access Point must be set to a country.

The export function will always export the encrypted Admin User password. The import function will import the Admin Password only if the Access Point is set to factory default. If the Access Point is not configured to factory default settings, the Admin User password WILL NOT get imported.

NOTE

Though the access point can have its basic settings defined using a number of different screens, Extreme Networks recommends using the access point Quick Setup screen to set the correct country of operation and define its minimum required configuration from one convenient location.

Configuring Device Settings

Configure a set of minimum required device settings within the *Quick Setup* screen. The values (LAN, WAN etc.) can often be defined in other locations within the menu tree. When you change the settings in the Quick Setup screen, the values also change within the screen where these parameters also exist. Additionally, if the values are updated in these other screens, the values initially set within the Quick Setup screen will be updated.

NOTE

A scheme for radio configuration and WIPS server management has been added within the Quick Setup GUI applet. Up to eight radio buttons are now available (depending on the number radios supported by the Access Point). These radio buttons define how WLAN and sensor functionality are supported amongst the radios available to the Access Point.

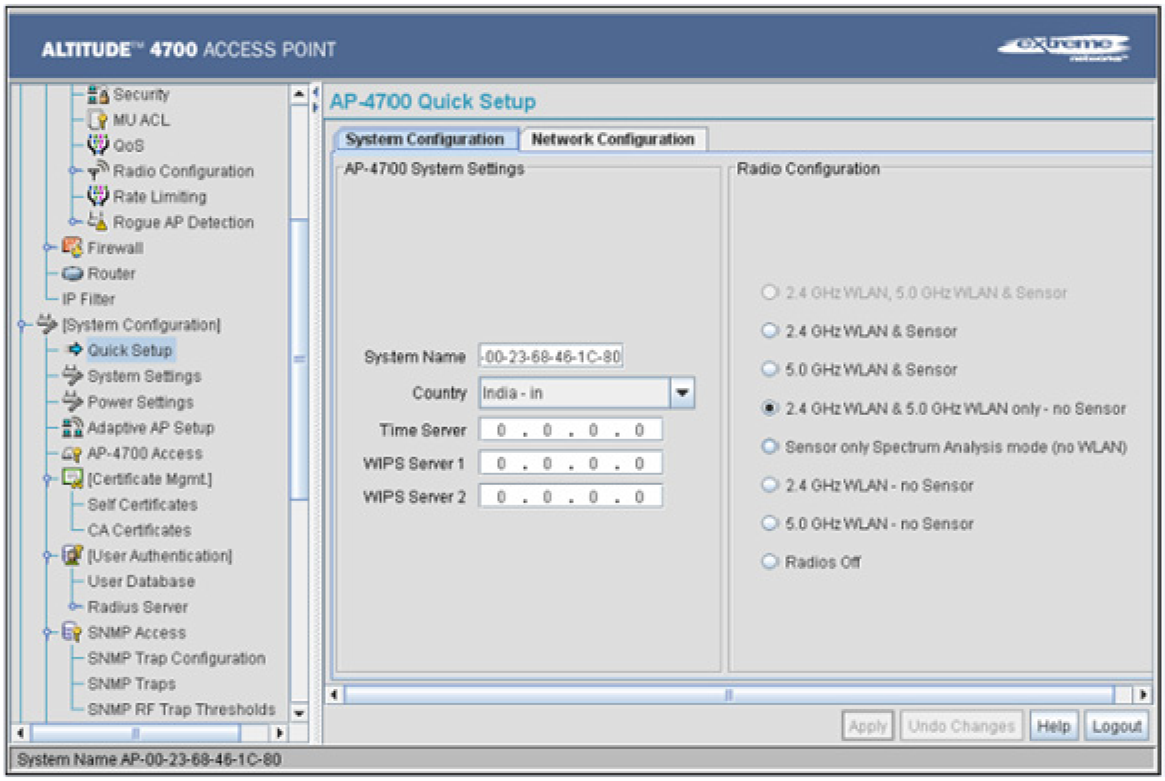
To define a basic Access Point configuration:

1 Select *System Configuration* > *Quick Setup* from the menu tree, if the Quick Setup screen is not already displayed.

2 Select the *System Configuration* tab to define the Access Point's system, WIPS server and radio configuration.

NOTE

The WIPS Server designation and radio configuration is defined as part of the Access Point's quick setup. For a description of sensor functionality and how it relates to Access Point operation, see "Sensor Support" on page 23.



AP-4700 System Settings

System Name: -00-23-68-46-1C-80

Country: India - in

Time Server: 0 . 0 . 0 . 0

WIPS Server 1: 0 . 0 . 0 . 0

WIPS Server 2: 0 . 0 . 0 . 0

Radio Configuration

○ 2.4 GHz WLAN, 5.0 GHz WLAN & Sensor

○ 2.4 GHz WLAN & Sensor

○ 5.0 GHz WLAN & Sensor

● 2.4 GHz WLAN & 5.0 GHz WLAN only - no Sensor

○ Sensor only Spectrum Analysis mode (no WLAN)

○ 2.4 GHz WLAN - no Sensor

○ 5.0 GHz WLAN - no Sensor

○ Radios Off

System Name AP-00-23-68-46-1C-80

3 Refer to the *AP4700 System Settings* field to define the following parameters:

System Name — Assign a *System Name* to define a title for this Access Point. The System Name is useful if multiple devices are being administered.

Country — Select the *Country* for the access point's country of operation. The Access Point prompts for the correct country code on the first login. A warning message also displays stating an incorrect country setting may result in illegal radio operation. Selecting the correct country is central to legally operating the Access Point. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted. To ensure compliance with national and local laws, set the country accurately. CLI and MIB users cannot configure their Access Point until a two character country code (for example, United States - us) is set.

Time Server — Optionally enter the IP address of the server used to provide system time to the access point within the *Time Server* field. Once the IP address is entered, the access point's *Network Time Protocol (NTP)* functionality is engaged automatically.

WIPS Servers — Define a primary and alternate WIPS server IP Address for WIPS Server 1 and 2. These are the addresses of the primary and secondary WIPS console server. WIPS support requires a Motorola AirDefense WIPS Server on the network. WIPS functionality is not provided by the Access Point alone. The Access Point works in conjunction with the dedicated WIPS server(s).

NOTE

The System Name and Country are also configurable within the System Settings screen. Refer to "Configuring System Settings" on page 78 (if necessary) to set a system location and admin email address for the access point or to view other default settings.

4 Refer to the new *Radio Configuration* field to define how WLAN and WIPS are supported by the Access Point's radio(s).

NOTE

If using the three radio Altitude 4750 Access Point, the radio three configuration option could be rendered unavailable if Rogue AP detection is enabled, or if the power source cannot provide adequate power for the third radio.

The Quick Setup screen on the previous page displays the Radio Configuration field with all 8 radio button options available. This is only the case with three radio Access Point SKUs. A dual radio model Access Point would display 7 of the eight possible configuration options. Refer to the following table for the options available to single, dual and three radio models.

Radio Button	Altitude 4710	Altitude 4750
2.4 GHz WLAN, 5.0 GHz WLAN & Sensor	Not Available	Radio 1 WLAN, Radio 2 WLAN, Radio 3 WIPS
2.4 GHz WLAN, & Sensor	Radio1 WLAN, Radio 2 WIPS	Radio 1 WLAN, Radio 2 WIPS, Radio 3 WIPS
5.0 GHz WLAN & Sensor	Radio 1 WIPS, Radio 2 WLAN	Radio 1 WIPS, Radio 2 WLAN, Radio 3 WIPS

Radio Button	Altitude 4710	Altitude 4750
2.4 GHz WLAN & 5.0 GHz WLAN only - no Sensor	Radio 1 WLAN, Radio 2 WLAN	Radio 1 WLAN, Radio 2 WLAN, Radio 3 Disabled
Sensor only Spectrum Analysis mode (no WLAN)	Radio 1 WIPS, Radio 2 WIPS	Radio 1 WIPS, Radio 2 WIPS, Radio 3 Disabled
2.4 GHz WLAN - no Sensor	Radio1 WLAN, Radio 2 Disabled	Radio 1 WLAN, Radio 2 Disabled, Radio 3 Disabled
5.0 GHz WLAN - no Sensor	Radio1 Disabled, Radio 2 WLAN	Radio 1 Disabled, Radio 2 WLAN, Radio 3 Disabled
Radios Off	Radios 1 and 2 Disabled	Radios 1, 2 and 3 Disabled

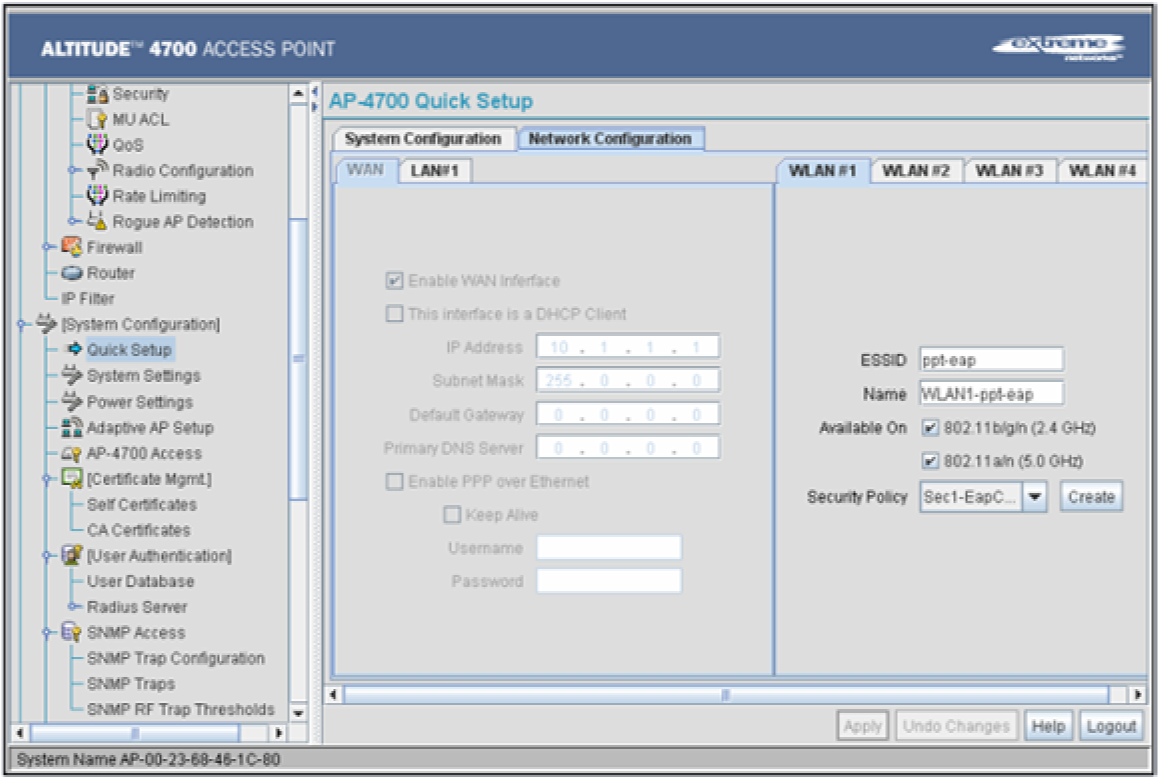
NOTE

If an Access Point transitions from a one-wlan-radio configuration to a two-wlan-radio config, the radio's previous user set values (like maximum MUs on radio) are not remembered and need to be defined again.

CAUTION

Only a qualified wireless network administrator should set the Access Point radio configuration. Refer to "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174 for an understanding of additional radio values and their implications.

5 Select the Quick Setup screen's *Network Configuration* tab to define a minimum set of WAN or LAN configuration values. The WAN tab displays by default.



☑ Enable WAN Interface

□ This interface is a DHCP Client

IP Address: 10 . 1 . 1 . 1

Subnet Mask: 255 . 0 . 0 . 0

Default Gateway: 0 . 0 . 0 . 0

Primary DNS Server: 0 . 0 . 0 . 0

□ Enable PPP over Ethernet

□ Keep Alive

Username:

Password:

ESSID: ppt-eap

Name: WLAN1-ppt-eap

Available On: ☑ 802.11b/g/n (2.4 GHz) ☑ 802.11a/n (5.0 GHz)

Security Policy: Sec1-EapC...

System Name AP-00-23-68-46-1C-80

Set a minimum set of parameters for using the WAN interface.

a Select the *Enable WAN Interface* checkbox to enable a connection between the access point and a larger network or outside world through the WAN port. Disable this option to effectively isolate the access point's WAN connection. No connections to a larger network or the Internet will be possible. MUs cannot communicate beyond the configured subnets.

b Select the *This Interface is a DHCP Client* checkbox to enable DHCP for the access point's WAN connection. This is useful, if the larger corporate network or *Internet Service Provider (ISP)* uses DHCP. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway.

NOTE

Extreme Networks recommends that the WAN and LAN ports should not be configured as DHCP clients at the same time.

c Specify an *IP address* for the access point's WAN connection. An IP address uses a series of four numbers expressed in dot notation, for example, 190.188.12.1 (no DNS names supported).

d Specify a *Subnet Mask* for the access point's WAN connection. This number is available from the ISP for a DSL or cable-modem connection, or from an administrator if the access point connects to a larger network. A subnet mask uses a series of four numbers expressed in dot notation. For example, 255.255.255.0 is a valid subnet mask.

e Define a *Default Gateway* address for the access point's WAN connection. The ISP or a network administrator provides this address.

f Specify the address of a *Primary DNS Server*. The ISP or a network administrator provides this address.

g Optionally, use the *Enable PPP over Ethernet* checkbox to enable *Point-to-Point Protocol over Ethernet (PPPoE)* for a high-speed connection that supports this protocol. Most DSL providers are currently using or deploying this protocol. PPPoE is a data-link protocol for dialup connections. PPPoE will allow the Access Point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data networks.

h Select the *Keep Alive* checkbox to enable occasional communications over the WAN port even when client communications to the WAN are idle. Some ISPs terminate inactive connections, while others do not. In either case, enabling Keep-Alive maintains the WAN connection, even when there is no traffic. If the ISP drops the connection after the idle time, the access point automatically reestablishes the connection to the ISP.

i Specify the *Username* entered when connecting to the ISP. When the Internet session begins, the ISP authenticates the username.

j Specify the *Password* entered when connecting to the ISP. When the Internet session starts, the ISP authenticates the password.

For additional access point WAN port configuration options, see "Configuring WAN Settings" on page 135.

6 Select the *LAN#1* tab to set a minimum set of parameters to use the LAN#1 interface.

a Select the *Enable LAN Interface* checkbox to forward data traffic over the access point's LAN connection. The LAN connection is enabled by default.

b Use the *This Interface* drop-down menu to specify how network address information is defined over the LAN connection. Select *DHCP Client* if the larger corporate network uses DHCP. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway. Select *DHCP Server* to use the access point as a DHCP server over the LAN connection. Select the *Bootp client* option to enable a diskless system to discover its own IP address.

NOTE

Extreme Networks recommends that the WAN and LAN ports should not both be configured as DHCP clients.

c Enter the network-assigned *IP Address* of the access point.

NOTE

DNS names are not supported as a valid IP address for the access point. The user is required to enter a numerical IP address.

d The *Subnet Mask* defines the size of the subnet. The first two sets of numbers specify the network domain, the next set specifies the subset of hosts within a larger network. These values help divide a network into subnetworks and simplify routing and data transmission.

e If using the static or DHCP Server option, enter a *Default Gateway* to define the numerical IP address of a router the access point uses on the Ethernet as its default gateway.

f If using the static or DHCP Server option, enter the *Primary DNS Server* numerical IP address.

g If using the DHCP Server option, use the *Address Assignment Range* parameter to specify a range of IP address reserved for mapping clients to IP addresses. If a manually (static) mapped IP address is within the IP address range specified, that IP address could still be assigned to another client. To avoid this, ensure all statically mapped IP addresses are outside of the IP address range assigned to the DHCP server.

For additional access point LAN port configuration options, see "Configuring the LAN Interface" on page 123.

7 Select the *WLAN #1* tab (WLANs 1 - 4 are available within the Quick Setup screen) to define its ESSID and security scheme for basic operation.

NOTE

A maximum of 16 WLANs are configurable within the Wireless Configuration screen.

a Enter the *Extended Services Set Identification (ESSID)* and name associated with the WLAN. For additional information on creating and editing up to 16 WLANs per access point, see "Creating/ Editing Individual WLANs" on page 148.

b Use the *Available On* checkboxes to define whether the target WLAN is operating in the 2.4 or 5 GHz radio band. Ensure the radio selected has been enabled (see step 8).

8 Once the WLAN's radio designations have been made, the radio must be configured in respect to intended 2.4 or 5 GHz radio traffic and the antennas used. Refer to *Network Configuration* > *Wireless* > *Radio Configuration* > *Radio1* (or *Radio2*), and configure the Radio Settings field (at a minimum). If you know the radio's Properties, Performance and Beacon Settings, those fields can also be defined at this time.

Define the Channel Settings, Power Level and 802.11 mode in respect to the 2.4 or 5 GHz 802.11b/g/n or 802.11a/n radio traffic and anticipated gain of the antennas.

CAUTION

Only a qualified wireless network administrator should set the Access Point radio configuration. Refer to "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174 for an understanding of additional radio values and their implications.

NOTE

Even an Access Point configured with minimal values must protect its data against theft and corruption. A security policy should be configured for WLAN1 as part of the basic configuration outlined in this guide. A security policy can be configured for the WLAN from within the Quick Setup screen. Policies can be defined over time and saved to be used as needed as security requirements change. Extreme Networks recommends you familiarize yourself with the security options available on the Access Point before defining a security policy. Refer to "Configuring Basic WLAN Security Settings" on page 73.

9 Click *Apply* to save any changes to the access point Quick Setup screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

10 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the access point Quick Setup screen to the last saved configuration.

Configuring Basic WLAN Security Settings

To configure a basic security policy for a WLAN:

1 From the Quick Setup screen, click the *Create* button to the right of the Security Policy item.

The *New Security Policy* screen displays with the *Manually Pre-shared key/No authentication* and *No Encryption* options selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a guest network wherein no sensitive data is either transmitted or received. Consequently, at a minimum, a basic security scheme (in this case WEP 128) is recommended in a network environment wherein sensitive data is transmitted.

NOTE

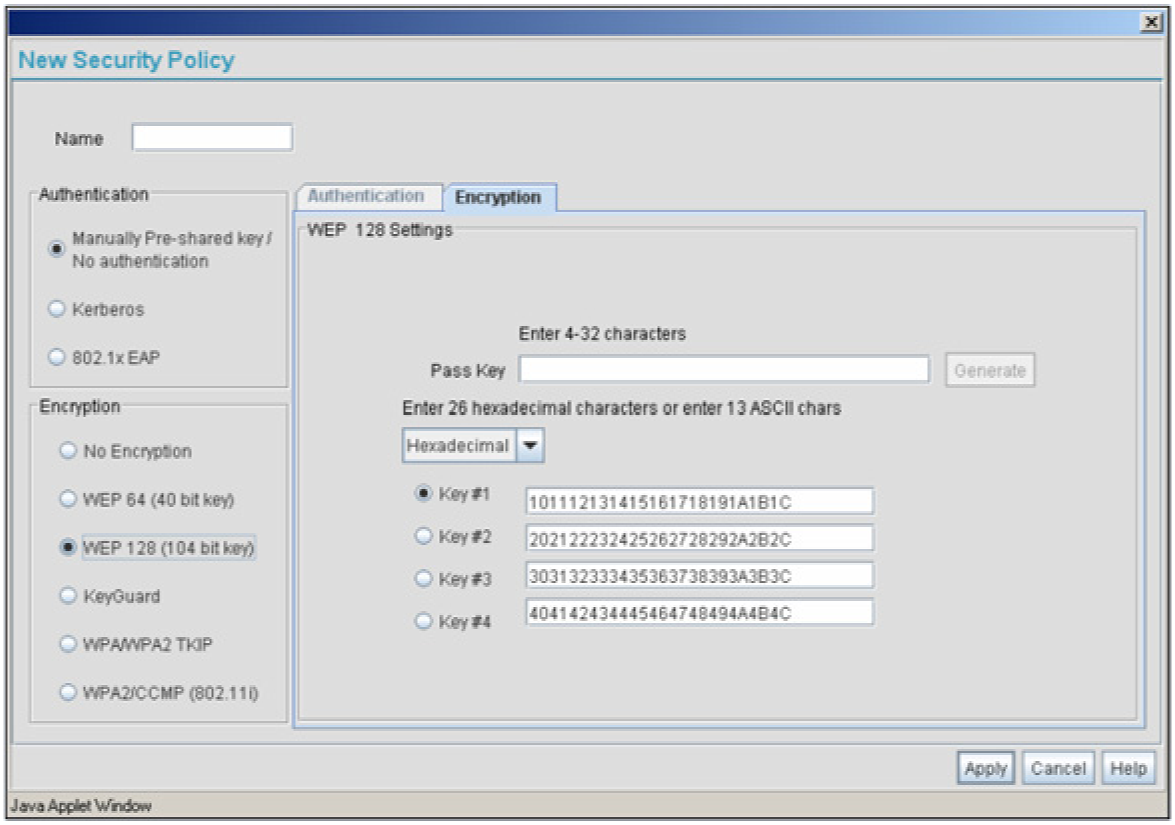
For information on configuring the other encryption and authentication options available to the access point, see "Configuring Security Options" on page 197.

2 Ensure the *Name* of the security policy entered suits the intended configuration or function of the policy.

Multiple WLANs can share the same security policy, so be careful not to name security policies after specific WLANs or risk defining a WLAN to single policy. Extreme Networks recommends naming the policy after the attributes of the authentication or encryption type selected.

3 Select the *WEP 128 (104 bit key)* checkbox.

The *WEP 128 Settings* field displays within the New Security Policy screen.



New Security Policy

Name

Authentication

● Manually Pre-shared key / No authentication

○ Kerberos

○ 802.1x EAP

Encryption

○ No Encryption

○ WEP 64 (40 bit key)

● WEP 128 (104 bit key)

○ KeyGuard

○ WPA/WPA2 TKIP

○ WPA2/CCMP (802.11i)

Authentication | Encryption

WEP 128 Settings

Enter 4-32 characters

Pass Key

Enter 26 hexadecimal characters or enter 13 ASCII chars

Hexadecimal

● Key #1 101112131415161718191A1B1C

○ Key #2 202122232425262728292A2B2C

○ Key #3 303132333435363738393A3B3C

○ Key #4 404142434445464748494A4B4C

4 Configure the *WEP 128 Settings* field as required to define the Pass Key used to generate the WEP keys.

Pass Key	Specify a 4 to 32 character pass key and click the *Generate* button. The Access Point, other proprietary routers and MUs use the same algorithm to convert a string to the same hexadecimal number. Motorola clients and devices need to enter WEP keys manually as hexadecimal numbers. The Access Point and its target client(s) must use the same pass key to interoperate.
Keys #1-4	Use the *Key #1-4* fields to specify key numbers. For WEP 64 (40-bit key), the keys are 10 hexadecimal characters in length. For WEP 128 (104-bit key), the keys are 26 hexadecimal characters in length. Select one of these keys for activation by clicking its radio button. The Access Point and its target client(s) must use the same key to interoperate.

5 Click the *Apply* button to save the security policy and return to the *Quick Setup* screen.

At this point, you can test the access point for MU interoperability.

Testing Connectivity

Verify the Access Point's link with an MU by sending *Wireless Network Management Protocol* (WNMP) ping packets to the associated MU. Use the Echo Test screen to specify a target MU and configure the parameters of the test. The WNMP ping test only works with certain Motorola MUs. Only use a Motorola MU to test Access Point connectivity using WNMP.

NOTE

Before testing for connectivity, the target MU needs to be set to the same ESSID as the Access Point. Since WEP 128 has been configured for the Access Point, the MU also needs to be configured for WEP 128 and use the same WEP keys. Ensure the MU is associated with the Access Point before testing for connectivity.

To ping a specific MU to assess its connection with an Access Point:

1 Select *Status and Statistics > MU Stats* from the menu tree.

2 Select the *Echo Test* button from within the *MU Stats Summary* screen.

3 Define the following parameters for the test.

Station Address	The station address is the IP address of the target MU. Refer to the MU Stats Summary screen for associated MU IP address information.
Number of pings	Defines the number of packets to be transmitted to the MU. The default is 100.
Packet Length	Specifies the length of each packet transmitted to the MU during the test. The default length is 100 bytes.

4 Click the *Ping* button to begin transmitting packets to the specified MU address.

Refer to the Number of Responses value to assess the number of responses from the MU versus the number of ping packets transmitted by the Access Point. Use the ratio of packets sent versus the number of packets received the link quality between the MU and the Access Point.

Click the *OK* button to exit the Echo Test screen and return to the MU Stats Summary screen.

Where to Go from Here?

Once basic connectivity has been verified, the access point can be fully configured to meet the needs of the network and the users it supports. Refer to the following:

- For detailed information on access point device access, SNMP settings, network time, importing/exporting device configurations and device firmware updates, see "System Configuration" on page 77.
- For detailed information on configuring access point LAN interface (subnet) and WAN interface see, "Network Management" on page 123.
- For detailed information on configuring specific encryption and authentication security schemes for individual access point WLANs, see "Configuring Access Point Security" on page 197.
- To view detailed statistics on the access point and its associated MUs, see "Monitoring Statistics" on page 263.

4

CHAPTER

System Configuration

The Access Point contains a built-in browser interface for system configuration and remote management using a standard Web browser such as Microsoft Internet Explorer, Netscape Navigator or Mozilla Firefox (version 0.8 or higher is recommended). The browser interface also allows for system monitoring of the Access Point.

Web management of the access point requires either Microsoft Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later.

NOTE

For optimum compatibility, use Sun Microsystems JRE 1.5 or higher (available from Sun's Web site), and be sure to disable Microsoft's Java Virtual Machine if installed.

To connect to the Access Point, an IP address is required. If connected to the Access Point using the WAN port, the default static IP address is 10.1.1.1. The default password is "*admin123*." If connected to the Access Point using the LAN port, the default setting is DHCP client. The user is required to know the IP address to connect to the Access Point using a Web browser.

System configuration topics include:

- Configuring System Settings on page 78
- Configuring Power Settings on page 81
- Adaptive AP Setup on page 85
- Configuring Data Access on page 87
- Managing Certificate Authority (CA) Certificates on page 91
- Configuring SNMP Settings on page 97
- Configuring LLDP Settings on page 108
- Configuring Network Time Protocol (NTP) on page 110
- Logging Configuration on page 112
- Importing/Exporting Configurations on page 114
- Updating Device Firmware on page 118

Configuring System Settings

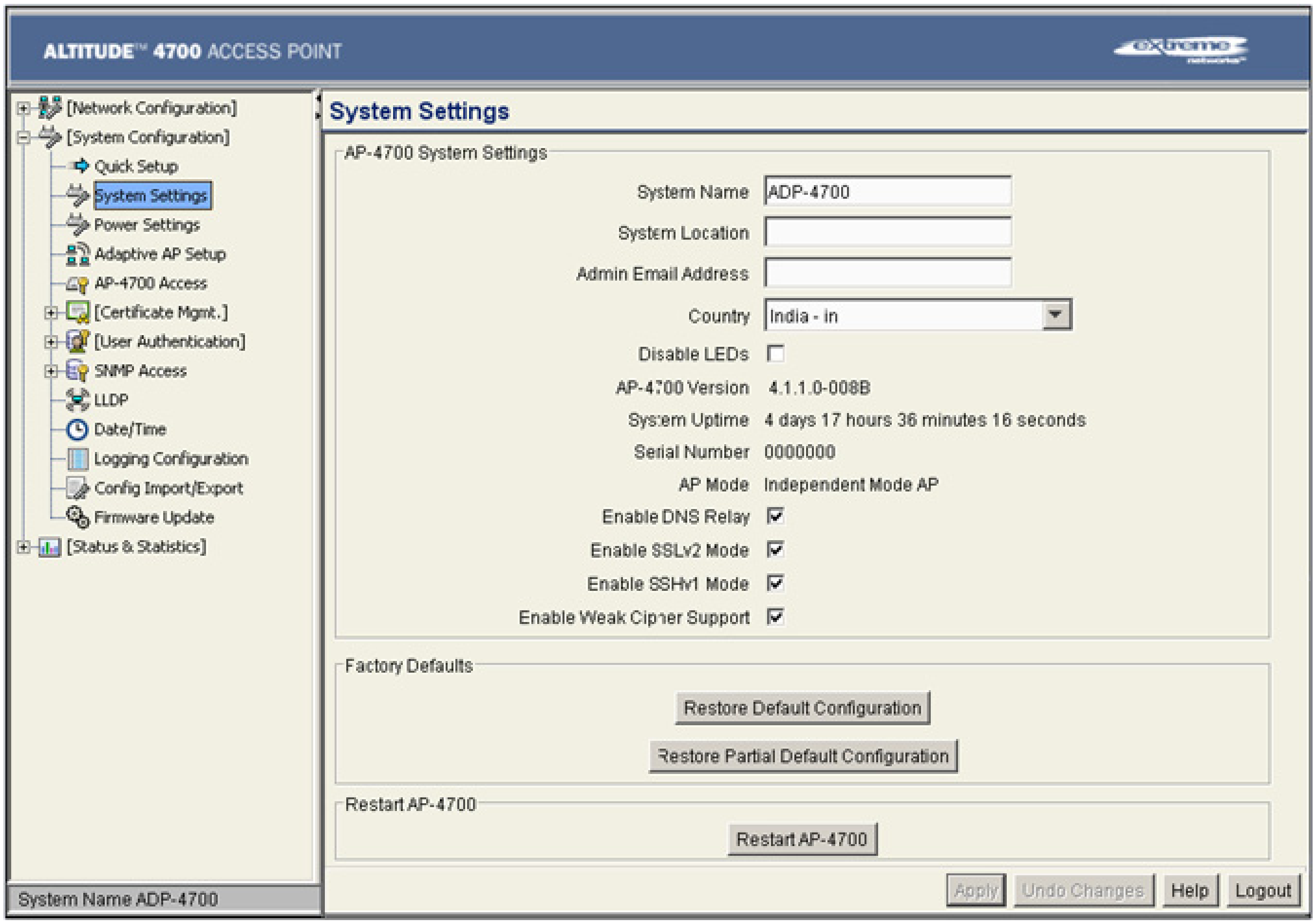
Use the *System Settings* screen to specify the name and location of the access point, assign an email address for the network administrator, restore the AP's default configuration, restart the AP or disable the Access Point's LEDs.

To configure System Settings for the access point:

CAUTION

The Access Point's country of operation is set from within the System Settings screen. If the country code is changed, the Access Point's power level, primary channel and secondary channel return to their default values. If changing the country code, be aware these values will require modification to their previous settings.

1 Select *System Configuration* > *System Settings* from the access point menu tree.



System Name ADP-4700

System Settings

AP-4700 System Settings

System Name	ADP-4700
System Location	
Admin Email Address	
Country	India - in
Disable LEDs	□
AP-4700 Version	4.1.1.0-008B
System Uptime	4 days 17 hours 36 minutes 16 seconds
Serial Number	0000000
AP Mode	Independent Mode AP
Enable DNS Relay	☑
Enable SSLv2 Mode	☑
Enable SSHv1 Mode	☑
Enable Weak Cipher Support	☑

Factory Defaults

Restart AP-4700

2 Configure the access point *System Settings* field to assign a system name and location, set the country of operation and view device version information.

System Name	Specify a device name for the access point. Extreme Networks recommends selecting a name serving as a reminder of the user base the access point supports (engineering, retail, etc.). This name will appear in the WIPS server when one of the radios is configured as a sensor and the WIPS functionality connects to the WIPS server. The WIPS module only accepts names with up to 20 characters, keep that if intending to use this AP as a sensor.
System Location	Enter the location of the access point. The *System Location* parameter acts as a reminder of where the AP can be found. Use the System Name field as a specific identifier of device location. Use the System Name and System Location fields together to optionally define the AP name by the radio coverage it supports and specific physical location. For example, “second floor engineering”
Admin Email Address	Specify the AP administrator's email address.
Country	The access point prompts the user for the correct country code after the first login. A warning message also displays stating that an incorrect country setting will lead to an illegal use of the Access Point. Use the pull-down menu to select the country of operation. Selecting the correct country is extremely important. Each country has its own regulatory restrictions concerning electromagnetic emissions (channel range) and the maximum RF signal strength transmitted. To ensure compliance with national and local laws, be sure to set the *Country* field correctly.
Disable LEDs	Select the *Disable LEDs* radio button to stop the Access Points LEDs from blinking during startup and normal operation. Selecting this option turns off all of the Access Point’s light pipes and none of the Access Point’s states are displayed by the LEDs. This option is disabled by default.
AP-4700 Version	The displayed number is the current version of the device firmware. Use this information to determine if the Access Point is running the most recent firmware available from Extreme Networks. Use the *Firmware Update* screen to keep the AP’s firmware up to date.
System Uptime	Displays the current uptime of the access point defined in the System Name field. *System Uptime* is the cumulative time since the access point was last rebooted or lost power.
Serial Number	Displays the access point *Media Access Control (MAC)* address. The access point MAC address is hard coded at the factory and cannot be modified. The LAN and WAN port MAC addresses can be located within the LAN and WAN Stats screens.
AP Mode	Displays the Access Point’s mode of operation to convey whether the Access Point is functioning as a standalone Access Point (Independent mode) or in Adaptive (thin AP) mode. If in Adaptive mode, the Access Point attempts to discover a controller through one or more of several mechanisms: DNS, DHCP, ICMP, CAPWAP or a statically programmed IP address.

Enable DNS Relay	Select the radio button to enable DNS relay. DNS relay is used to prevent access to the port used by DNS. If disabled, clients connected to the Access Point are not able to browse sites since DNS is disabled. This feature is enabled by default.
Enable SSLv2 Mode	Select the radio button to enable SSL (Secure Socket Layer) version 2 support. SSL provides session encryption and message authentication. This feature is enabled by default.
Enable SSHv1 Mode	Select the radio button to enable SSH version 1 support. Secure Shell (SSH) is a protocol that provides a secure, remote connection to an Access Point. This feature is enabled by default.
Enable Weak Cipher Support	Select the radio button to enable the Access Point to support SSL ciphers less than 128 bits in length. This feature is enabled by default.

3 Refer to the *Factory Defaults* field to restore either a full or partial default configuration.

CAUTION

Restoring the Access Point’s configuration back to default settings changes the administrative password back to “admin123” If restoring the configuration back to default settings, be sure you change the administrative password accordingly.

Restore Default Configuration	Select the *Restore Default Configuration* button to reset the AP’s configuration to factory default settings. If selected, a message displays warning the user the current configuration will be lost if the default configuration is restored. Before using this feature, Extreme Networks recommends using the *Config Import/Export* screen to export the current configuration for safekeeping.
Restore Partial Default Configuration	Select the *Restore Partial Default Configuration* button to restore a default configuration with the exception of the current LAN, WAN, SNMP settings and IP address used to launch the browser. If selected, a message displays warning the user all current configuration settings will be lost with the exception of WAN and SNMP settings. Before using this feature, Extreme Networks recommends using the *Config Import/Export* screen to export the current configuration for safekeeping.

4 Use the *Restart* access point field to restart the AP (if necessary).

Restart AP4700	Click the *Restart* access point button to reboot the AP. Restarting the access point resets all data collection values to zero. Extreme Networks does not recommend restarting the AP during significant system uptime or data collection activities.

CAUTION

After a reboot, static route entries disappear from the AP Route Table if a LAN Interface is set to DHCP Client. The entries can be retrieved (once the reboot is done) by performing an Apply operation from the WEB UI or a save operation from the CLI.

5 Click *Apply* to save any changes to the System Settings screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

NOTE

The Apply button is not needed for restoring the access point default configuration or restarting the access point.

6 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the System Settings screen to the last saved configuration.

7 Click *Logout* to securely exit the access point applet. A prompt displays confirming the logout before the applet is closed.

Configuring Power Settings

Use the *Power Setting* screen to select one of two power modes, *3af* or *Auto.* When automatic is selected, the Access Point safely operates within available power. Once the power configuration is determined, the Access Point configures its operating power characteristics based on its SKU and power configuration.

The Access Point uses a *complex programmable logic device* (CPLD). The CPLD determines proper supply sequencing, the maximum power available and other status information. One of the primary functions of the CPLD is to determine the Access Point's maximum power budget. When the AP is powered on (or performing a cold reset), the CPLD determines the maximum power provided by the POE device and the budget available to the Access Point. The CPLD also determines the Access Point hardware SKU and the number of radios. If the Access Point's POE resource cannot provide sufficient power to run the Access Point (with all intended interfaces enabled), some of the following interfaces could be disabled or modified:

- The Access Point's transmit and receive algorithms could be negatively impacted
- The Access Point's transmit power could be reduced due to insufficient power
- The Access Point's WAN port configuration could be changed (either enabled or disabled)

Automatic is the default mode. When Auto is selected, the CPLD determines how much power is available at startup, either 3af, Mid Power or Full Power for an Altitude 4710 or 3af, 3at or Full Power for an Altitude 4750 model. Based on the power level, the Access Point configures its power consumption based on the table below:

Altitude 4700 Available Power	**Altitude 4710 Operational Configuration**
13 watts (3af) *Power Status: 3af*	Two radios, processor running at 500 MHz, GE1 port (1000BASE-T) and GE2 port disabled.
18 watts *Power Status: Mid Power*	Two radios, processor running at 500 MHz, GE1 port (1000BASE-T) and GE2 port (100 BASE-T).
24 watts or external power supply *Power Status: Full Power*	Two radios, processor running at 500 MHz, GE1 port (1000BASE-T) and GE2 port (1000 BASE-T).

NOTE

An Altitude 4750 Access Point has different available power from an Altitude 4710 Access Point. An Altitude 4750 model uses 22 watts when its power status is 3af, 23 - 26 watts when its power status is 3at and 27 watts when its power status is Full Power.

CAUTION

The power modes described in the section are only obtainable using the 48-Volt Power Supply designed specifically for an Altitude 4700 Series Access Point.

NOTE

Radio transmit power is not used as one of the factors to determine the available power budget. If an external power supply is used, it is assumed it will provide full power. When operating using full power, each radio has 3x3 antenna mode support and its intended transmit power budget.

Radios at Full Power

The table below describes the maximum transmit power available to each radio (at varying data rates) when the Access Point is receiving full DC power and is not compromised in its power budget. These values should be viewed as the safe limit for the Access Point's radio at full power and should not be exceeded.

Rates (Mbps)	MCS Indices	EVM	Bandwidth	Maximum Transmit Power 2.4 GHz	Maximum Transmit Power 5 GHz
1		-9	20MHz	23	NA
2		-9	20MHz	23	NA
5.5		-9	20MHz	23	NA
11		-9	20MHz	23	NA
6		-5	20MHz	23	20
9		-8	20MHz	23	20
12		-10	20MHz	23	20
18		-13	20MHz	23	20
24		-16	20MHz	22	20
36		-19	20MHz	22	19
48		-22	20MHz	21	18
54		-25	20MHz	20	17
	MCS0/MCS8	-5	HT20/40	23	20
	MCS1/MCS9	-10	HT20/40	23	20
	MCS2/MCS10	-13	HT20/40	23	20
	MCS3/MCS11	-16	HT20/40	23	19
	MCS4/MCS12	-19	HT20/40	22	19
	MCS5/MCS13	-22	HT20/40	22	18

Rates (Mbps)	MCS Indices	EVM	Bandwidth	Maximum Transmit Power 2.4 GHz	Maximum Transmit Power 5 GHz
	MCS6/MCS14	-25	HT20/40	21	17
	MCS7/MCS15	-28	HT20/40	20	17

Radios at Low Power

The table below describes the maximum transmit power available to each radio (at varying data rates) when the Access Point is receiving low DC power in either af or at mode.

CAUTION

Exceeding the limits listed below can cause damage to the Access Point or cause the radio to operate unpredictably. Thus, these values should be viewed as the safe limit for the Access Point's radio and should not be exceeded in either af or at mode.

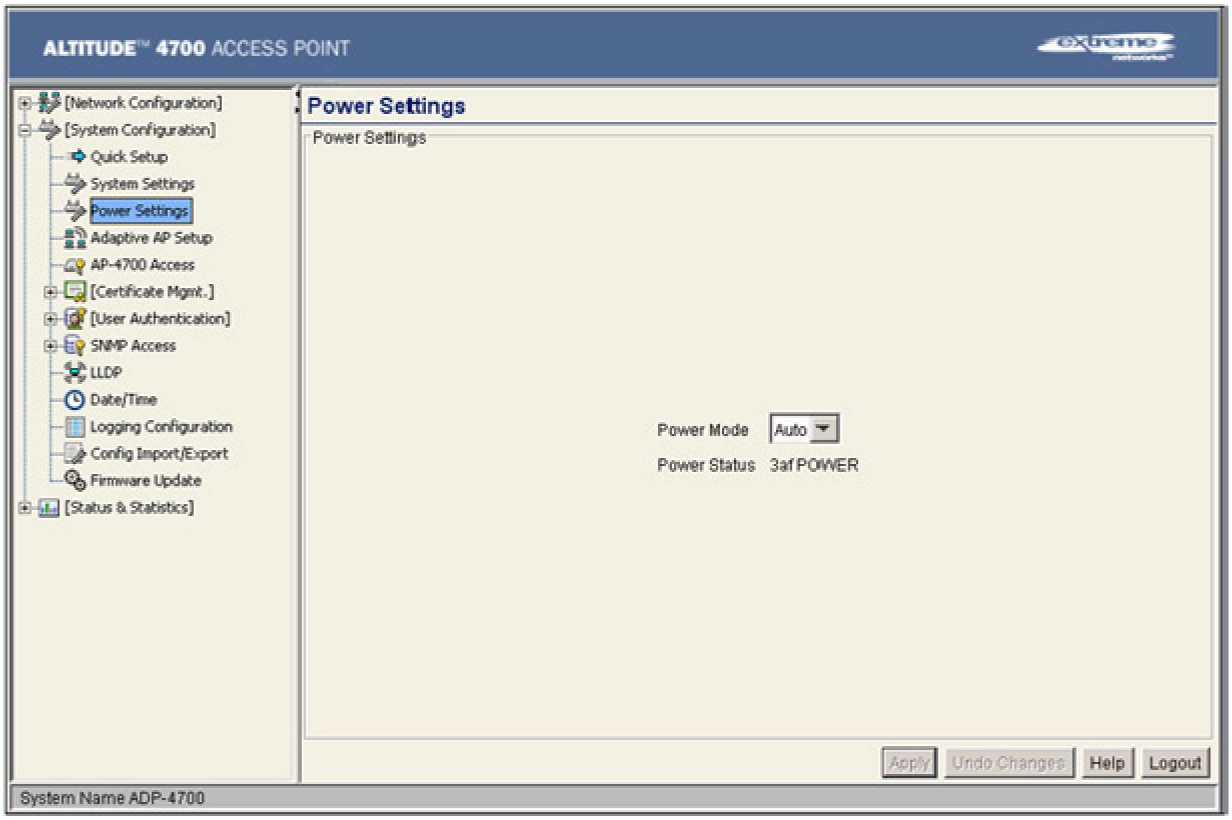
Rates (Mbps)	MCS Indices	EVM	Bandwidth	Maximum Transmit Power 2.4 GHz	Maximum Transmit Power 5 GH
1		-9	20MHz	20	NA
2		-9	20MHz	20	NA
5.5		-9	20MHz	20	NA
11		-9	20MHz	20	NA
6		-5	20MHz	22	19
9		-8	20MHz	22	19
12		-10	20MHz	22	19
18		-13	20MHz	22	18
24		-16	20MHz	21	18
36		-19	20MHz	20	17
48		-22	20MHz	18	15
54		-25	20MHz	17	13
	MCS0/MCS8	-5	HT20/40	22	19
	MCS1/MCS9	-10	HT20/40	22	19
	MCS2/MCS10	-13	HT20/40	21	18
	MCS3/MCS11	-16	HT20/40	21	17
	MCS4/MCS12	-19	HT20/40	20	17
	MCS5/MCS13	-22	HT20/40	19	16
	MCS6/MCS14	-25	HT20/40	18	15
	MCS7/MCS15	-28	HT20/40	17	15

NOTE

The Access Point could allow the operation of only one radio depending on the POE power level provided. When only one radio is operational, it is configured as either a WIPS or WLAN radio. Consequently, if the Access Point transitions from dual to single radio operation, a WIPS radio might not be available.

To define the Access Point's power setting:

1 Select *System Configuration* > *Power Settings* from the menu tree.



Power Settings

Power Settings

Power Mode: Auto

Power Status: 3af POWER

System Name ADP-4700

2 Refer to the following to assess the Access Point's current power state. Once known, determine how available power resources are applied to the Access Point's radios.

NOTE

Within the Power Configuration field, an installation professional selects a power mode based on the different power resources available to that Access Point. For 3af and 3at, choose between Default and Option as best suited to that hardware. For example, if Option is selected for 3af Power, and the Access Point is a dual radio model, the following configuration is set:

LAN port ON (1000 BAST-T)
WAN port OFF
Radio 1 (2.4) on, 2x3 mode with maximum transmit power 18dBm
Radio 2 (5.0) on, 2x3 mode with maximum transmit power 18dBm

Contact Extreme Networks Support if unsure of your Access Point's optimal power management settings. Go to https://esupport.extremenetworks.com.

Power Status

Refer to the (read only) power status field to review the power available to the AP. The status for an Altitude 4710 and Altitude 4750 are slightly different. For an Altitude 4710, the options are 3af, Mid Power or Full Power. For an Altitude 4750 model, the options are 3at, 3af or Full Power.

Power Mode	When the Access Point is powered on for the first time, the system determines the power budget available to the Access Point. Using the *Auto* setting (default setting), the Access Point automatically determines the best power configuration based on the available power budget. If *3af* is selected, the AP assumes 12.95 watts are available. If the mode is changed, the Access Point requires a reset to implement the change.
3af Power	If 3af is selected, the AP is configured assuming 12.95 watts are available using a 3af power budget, even though there may actually be more power available. Set the 3af Power to either Default or Option. Changing the power option to 3af restarts the Access Point in order to implement the change. The Access Point's WAN port is turned off if the power mode is set to 3af.
3at Power	Set the power option for 3at to either Default or Option. Changing the power option to 3at restarts the Access Point in order to implement the change. With 3at power, both Ethernet ports are available using 1000BAST-T mode.
Default Radio	Define whether radio 1 or radio 2 is the default radio.With three radio models, this is especially important when the power budget can only accommodate one radio to be optimally powered. If using a dual radio Access Point, power is negotiated between the radios per the defined configuration. If deploying a three radio model Altitude 4750, the third radio can never be the default radio.

3. Click *Apply* to save any changes to the Power Settings screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.
4. Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Power Settings screen to the last saved configuration.
5. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Adaptive AP Setup

An Access Point needs settings defined to discover (and adopt) an available controller and establish a connection and data tunnel. It's through this controller adoption that the Access Point receives its *adaptive AP* (AAP) configuration. The Access Point has a screen to define the mechanisms used to adopt a controller and route AAP configuration information.

NOTE

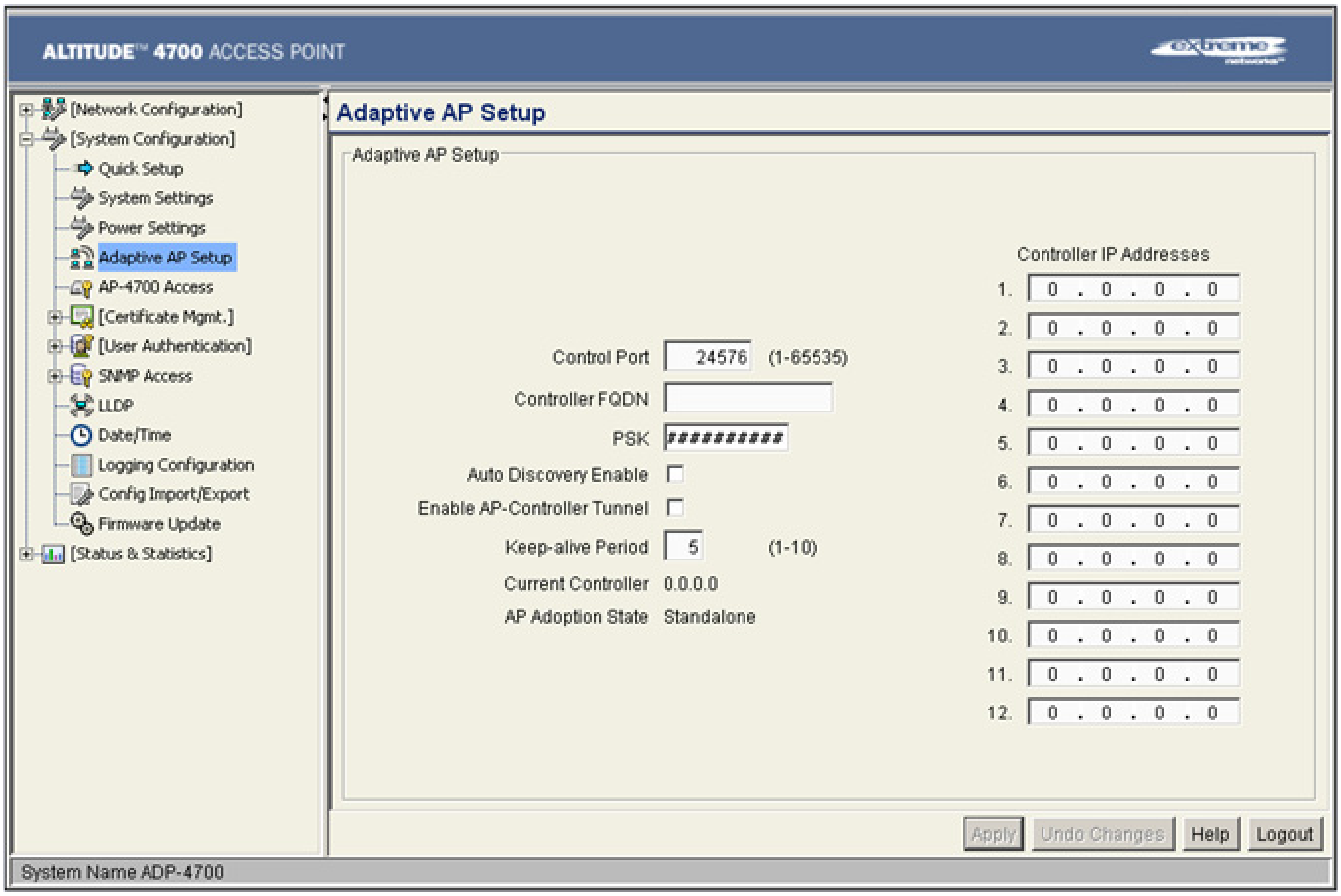
For an AAP overview and a theoretical discussion of how an Access Point discovers a controller to create a secure data tunnel for adaptive AP operation, see "Adaptive AP" on page 605.

NOTE

The Adaptive AP Setup screen does not display the AAP's adoption status or adopted controller. This information is available using the Access Point's CLI.

To configure the Access Point's controller discovery method and connection medium:

1 Select *System Configuration > Adaptive AP Setup* from the menu tree.



Adaptive AP Setup

Adaptive AP Setup

Control Port	24576 (1-65535)
Controller FQDN	
PSK	###########
Auto Discovery Enable	□
Enable AP-Controller Tunnel	□
Keep-alive Period	5 (1-10)
Current Controller	0.0.0.0
AP Adoption State	Standalone

Controller IP Addresses

1.	0 . 0 . 0 . 0
2.	0 . 0 . 0 . 0
3.	0 . 0 . 0 . 0
4.	0 . 0 . 0 . 0
5.	0 . 0 . 0 . 0
6.	0 . 0 . 0 . 0
7.	0 . 0 . 0 . 0
8.	0 . 0 . 0 . 0
9.	0 . 0 . 0 . 0
10.	0 . 0 . 0 . 0
11.	0 . 0 . 0 . 0
12.	0 . 0 . 0 . 0

System Name ADP-4700

2 Define the following to prioritize a controller connection scheme and AP interface used to adopt to the controller.

Control Port — Define the port used by the controller FQDN to transmit and receive with the AAP. The default control port is 24576.

Controller FQDN — Add a complete controller *fully qualified domain name* (FQDN) to add a controller to the 12 available controller IP addresses available for connection. The Access Point resolves the name to one or more IP addresses if a DNS IP address is present. This method is used when the Access Point fails to obtain an IP address using DHCP.

PSK — Before the Access Point sends a packet requesting its mode and configuration, the controller and the Access Point require a secure link using a pre-shared key.

Auto Discovery Enable — When the *Auto Discovery Enable* checkbox is selected, the Access Point begins the controller discovery (adoption) process using DHCP first, then a user provided domain name, lastly using static IP addresses. This setting is disabled by default. When disabled, the AP functions as a standalone Access Point without trying to adopt a controller. Consequently, the Access Point will not be able to obtain an AAP configuration.

Enable AP-Controller Tunnel	This setting is required to enable an IPSec VPN from the AAP to the Wireless Controller.
Keep-alive Period	The Keepalive interval defines a period (in seconds) the AAP uses to terminate its connection to the controller if no data is received.
Current Controller	Displays the IP address of the connected controller. This is the controller from which the Access Point receives its adaptive configuration.
AP Adoption State	Displays whether the Access Point has been adopted by the controller (whose IP address is listed in the Current Controller parameter). The Access Point cannot receive its adaptive configuration without association. A stand-alone Access Point can be adopted by a wireless controller. A stand-alone AP also supports operations without being adopted by a controller.

3 Refer to the 12 available *Controller IP Addresses* to review the addresses the Access Point uses to adopt with a controller.

The Access Point contacts each controller on the list (from top to bottom) until a viable controller adoption is made. The Access Point first populates the list with the IP addresses received from its DHCP resource. If DHCP is not able to obtain IP addresses, the Access Point attempts to resolve the controller's Domain Name if provided within the Controller FQDN parameter. However, if the Access Point receives one or more IP addresses from the DHCP server, it will not solicit an IP address from a user provided domain name. Lastly, provide static (manually provided) IP addresses to the list as long as there is room. The Access Point will defer to these addresses if DHCP and a provided domain address fail to secure a controller adoption.

4 Click *Apply* to save any changes to the Adaptive AP Setup screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

5 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Adaptive AP Setup screen to the last saved configuration.

6 Click *Logout* to securely exit the access point applet. A prompt displays confirming the logout before the applet is closed.

Configuring Data Access

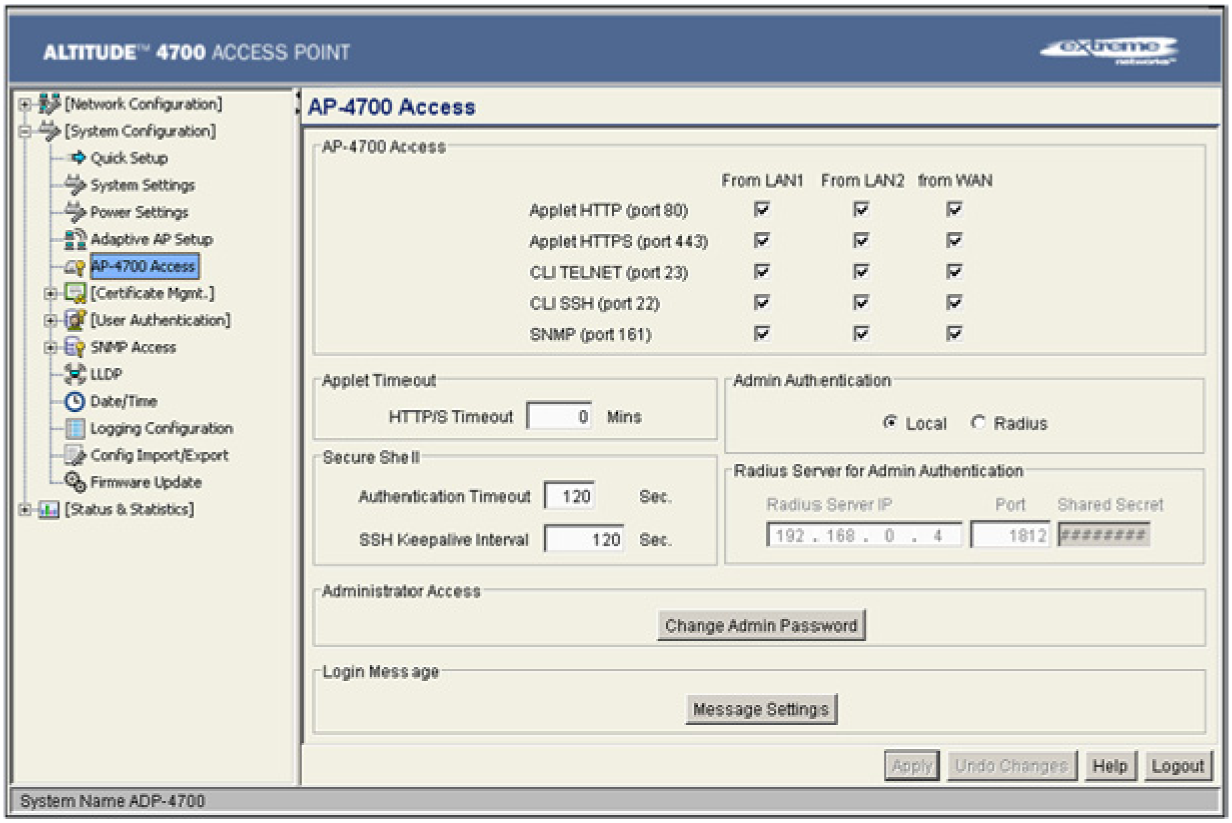
Use the *AP4700 Access* screen to allow/deny management access to the Access Point from different subnets (LAN1, LAN2 or WAN) using different protocols such as HTTPS, Telnet, SSH or SNMP. The access options are either enabled or disabled. It is not meant to function as an ACL in routers or other firewalls, where you can specify and customize specific IPs to access specific interfaces.

Use the Access screen checkboxes to enable or disable LAN1, LAN2 and/or WAN access using the protocols and ports listed. If access is disabled, this effectively locks out the administrator from configuring the access point using that interface. To avoid jeopardizing the network data managed by the access point, Extreme Networks recommends enabling only those interfaces used in the routine (daily) management of the network, and disabling all other interfaces until they are required.

The Access screen also has a new facility allowing customers to create a login message with customer generated text. When enabled (using either the Access Point Web UI or CLI), the login message displays when the user is logging into the Access Point. If the login message is disabled, the default login screen displays with no message.

To configure access for the access point:

1 Select *System Configuration* > *AP4700 Access* from the menu tree.



AP-4700 Access

AP-4700 Access

	From LAN1	From LAN2	from WAN
Applet HTTP (port 80)	☑	☑	☑
Applet HTTPS (port 443)	☑	☑	☑
CLI TELNET (port 23)	☑	☑	☑
CLI SSH (port 22)	☑	☑	☑
SNMP (port 161)	☑	☑	☑

Applet Timeout

HTTP/S Timeout 0 Mins

Admin Authentication

● Local ○ Radius

Secure Shell

Authentication Timeout 120 Sec.

SSH Keepalive Interval 120 Sec.

Radius Server for Admin Authentication

Radius Server IP 192 . 168 . 0 . 4 Port 1812 Shared Secret ########

Administrator Access

Login Message

System Name ADP-4700

2 Use the *AP4700 Access* field checkboxes to enable/disable the following on the Access Point's LAN1, LAN2 or WAN interfaces:

Applet HTTP (port 80)	Select the LAN1, LAN2 and/or WAN checkboxes to enable access to the access point configuration applet using a Web browser.
Applet HTTPS (port 443)	Select the LAN1, LAN2 and/or WAN checkboxes to enable access to the access point configuration applet using a *Secure Sockets Layer (SSL)* for encrypted HTTP sessions.
CLI TELNET (port 23)	Select the LAN1, LAN2 and/or WAN checkboxes to enable access to the access point CLI via the TELNET terminal emulation TCP/IP protocol.
CLI SSH (port 22)	Select the LAN1, LAN2 and/or WAN checkboxes to enable access to the access point CLI using the SSH (Secure Shell) protocol.
SNMP (port 161)	Select the LAN1, LAN2 and/or WAN checkboxes to enable access to the access point configuration settings from an SNMP-capable client.

3 Refer to the *Applet Timeout* field to set an HTTPS timeout interval.

HTTP/S Timeout	Disables access to the Access Point if no data activity is detected over Applet HTTPS (port 443) after the user defined interval. Default is 0 Mins.

4 Configure the *Secure Shell* field to set timeout values to reduce network inactivity.

Authentication Timeout
Defines the maximum time (between 30 - 120 seconds) allowed for SSH authentication to occur before executing a timeout. The minimum permissible value is 30 seconds.

SSH Keepalive Interval
The SSH Keepalive Interval defines a period (in seconds) after which if no data has been received from a client, SSH sends a message through the encrypted channel to request a response from the client. The default is 0, and no messages will be sent to the client until a non-zero value is set. Defining a Keepalive interval is important, otherwise programs running on a server may never notice if the other end of a connection is rebooted.

5 Use the *Admin Authentication* buttons to specify the authentication server connection method.

Local
The access point verifies the authentication connection.

Radius
Designates that a RADIUS server is used in the authentication credential verification. If using this option, the connected PC is required to have its RADIUS credentials verified with an external RADIUS server. Additionally, the RADIUS Server's Active Directory should have a valid user configured and have a PAP based Remote Access Policy configured for RADIUS Admin Authentication to work.

6 Use the RADIUS Server if a RADIUS server has been selected as the authentication server. Enter the required network address information.

Radius Server IP
Specify the numerical (non DNS name) IP address of the *Remote Authentication Dial-In User Service* (RADIUS) server. RADIUS is a client/server protocol and software enabling remote-access servers to communicate with a server used to authenticate users and authorize access to the requested system or service.

Port
Specify the port on which the server is listening. The RADIUS server typically listens on ports 1812 (default port).

Shared Secret
Define a shared secret for authentication on the server. The shared secret is required to be the same as the shared secret defined on the RADIUS server. Use shared secrets to verify RADIUS messages (with the exception of the Access-Request message) sent by a RADIUS-enabled device configured with the same shared secret.

Apply the qualifications of a well-chosen password to the generation of a shared secret. Generate a random, case-sensitive string using letters and numbers. The default is admin123.

7 Update the *Administrator Access* field to change the administrative password used to access the configuration settings.

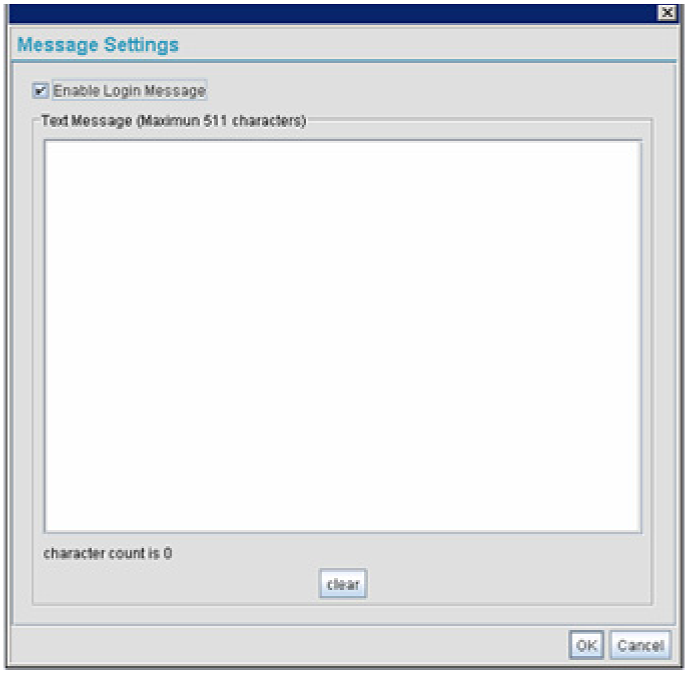
Change Admin Password
Click the *Change Admin Password* button to display a screen for updating the AP administrator password. Enter and confirm a new administrator password as required.

8 Refer to the *Login Message* field to optionally define a message displayed to the customer as they login into the Access Point.

Message Settings

Click the *Message Settings* button to display a screen used to create a text message. Once displayed, select the *Enable Login Message* checkbox to allow your customized message to be displayed when the user is logging into the Access Point. If the checkbox is not selected (as is the case by default), the user will encounter the login screen with no additional message.

When the login message function is enabled, the user can enter a (511 character maximum) message describing any usage caveat required (such as the authorization disclaimer displayed on the following page). Thus, the login message can serve an important function by discouraging unauthorized users from illegally managing the Access Point. As your message is entered, the character usage counter is updated to allow you to visualize how close you are coming to the maximum allowed number of characters. Click the *Clear* button at any time to remove the contents of the message and begin a new one. Once you have finished creating your message, click the *OK* button to return to the Access screen.



☑ Enable Login Message

character count is 0

9 Click *Apply* to save any changes to the Access screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

10 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Access screen to the last saved configuration.

11 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Managing Certificate Authority (CA) Certificates

Certificate management includes the following sections:

- Importing a CA Certificate on page 91
- Creating Self Certificates for Accessing the VPN on page 92

Importing a CA Certificate

A *certificate authority (CA)* is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates that it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain this CA certificate in its *Trusted Root Library* so it can trust certificates “signed” by the CA's private key.

Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information.

The access point can import and maintain a set of CA certificates to use as an authentication option for *Virtual Private Network* (VPN) access. To use the certificate for a VPN tunnel, define a tunnel and select the IKE settings to use either RSA or DES certificates. For additional information on configuring VPN tunnels, see “Configuring VPN Tunnels” on page 225.

CAUTION

Loaded and signed CA certificates will be lost when changing the Access Point’s firmware version using either the GUI or CLI. After a certificate has been successfully loaded, export it to a secure location to ensure its availability after a firmware update.

If restoring the Access Point’s factory default firmware, you must export the certificate file BEFORE restoring the Access Point’s factory default configuration. Import the file back after the updated firmware is installed.

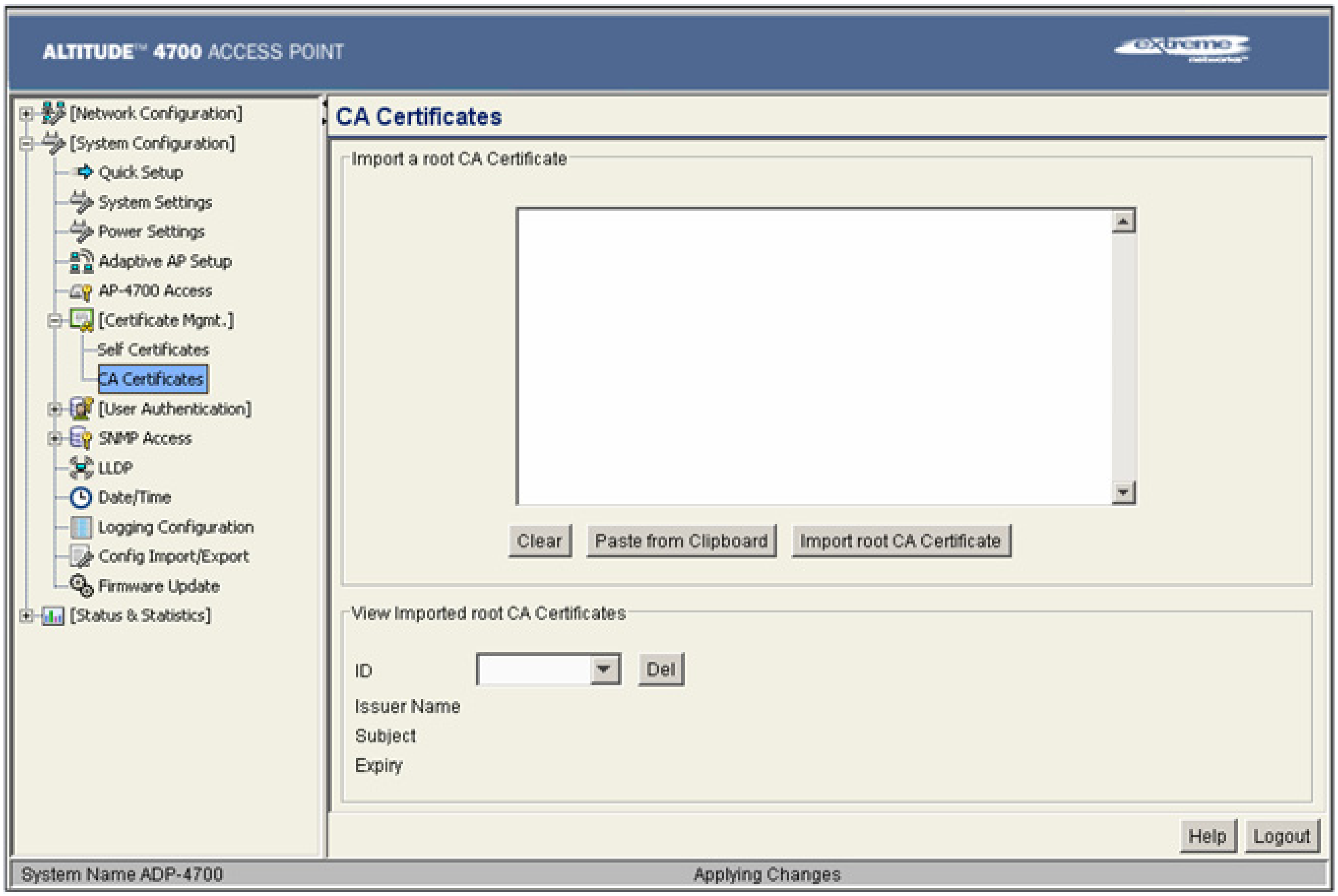
Refer to your network administrator to obtain a CA certificate to import into the access point.

NOTE

Verify the access point device time is synchronized with an NTP server before importing a certificate to avoid issues with conflicting date/time stamps. For more information, see “Configuring Network Time Protocol (NTP)” on page 110.

To import a CA certificate:

1 Select *System Configuration* > *Certificate Mgmt* > *CA Certificates* from the menu tree.



2 Copy the content of the CA Certificate message (using a text editor such as notepad) and click on *Paste from Clipboard*.

The content of the certificate displays in the *Import a root CA Certificate* field.

3 Click the *Import root CA Certificate* button to import it into the CA Certificate list.

4 Once in the list, select the certificate ID within the *View Imported root CA Certificates* field to view the certificate issuer name, subject, and certificate expiration data.

5 To delete a certificate, select the Id from the drop-down menu and click the *Del* button.

Creating Self Certificates for Accessing the VPN

The access point requires two kinds of certificates for accessing the VPN, CA certificates and self certificates. Self certificates are certificate requests you create, send to a *Certificate Authority* (CA) to be signed, then import the signed certificate into the management system.

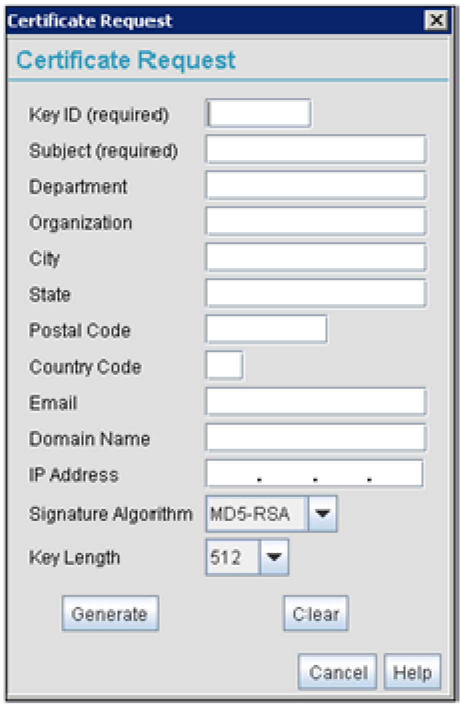
CAUTION

Self certificates can only be generated using the Access Point GUI and CLI interfaces. No functionality exists for creating a self-certificate using the Access Point's SNMP configuration option.

To create a self certificate:

1 Select *System Configuration > Certificate Mgmt > Self Certificates* from the access point menu tree.

2 Click on the *Add* button to create the certificate request.



Certificate Request

Certificate Request

Key ID (required)

Subject (required)

Department

Organization

City

State

Postal Code

Country Code

Email

Domain Name

IP Address . . .

Signature Algorithm MD5-RSA

Key Length 512

The *Certificate Request* screen displays.

3 Complete the request form with the pertinent information. Only 4 values are required, the others optional.

Key ID

Enter a logical name for the certificate to help distinguish between certificates. The name can be up to 7 characters in length.

Subject

The required *Subject* value contains important information about the certificate. Contact the CA signing the certificate to determine the content of the Subject parameter.

Signature Algorithm

Use the drop-down menu to select the signature algorithm used for the certificate. Options include:

- *MD5-RSA*—Message Digest 5 algorithm in combination with RSA encryption.
- *SHA1-RSA*—Secure Hash Algorithm 1 in combination with RSA encryption.

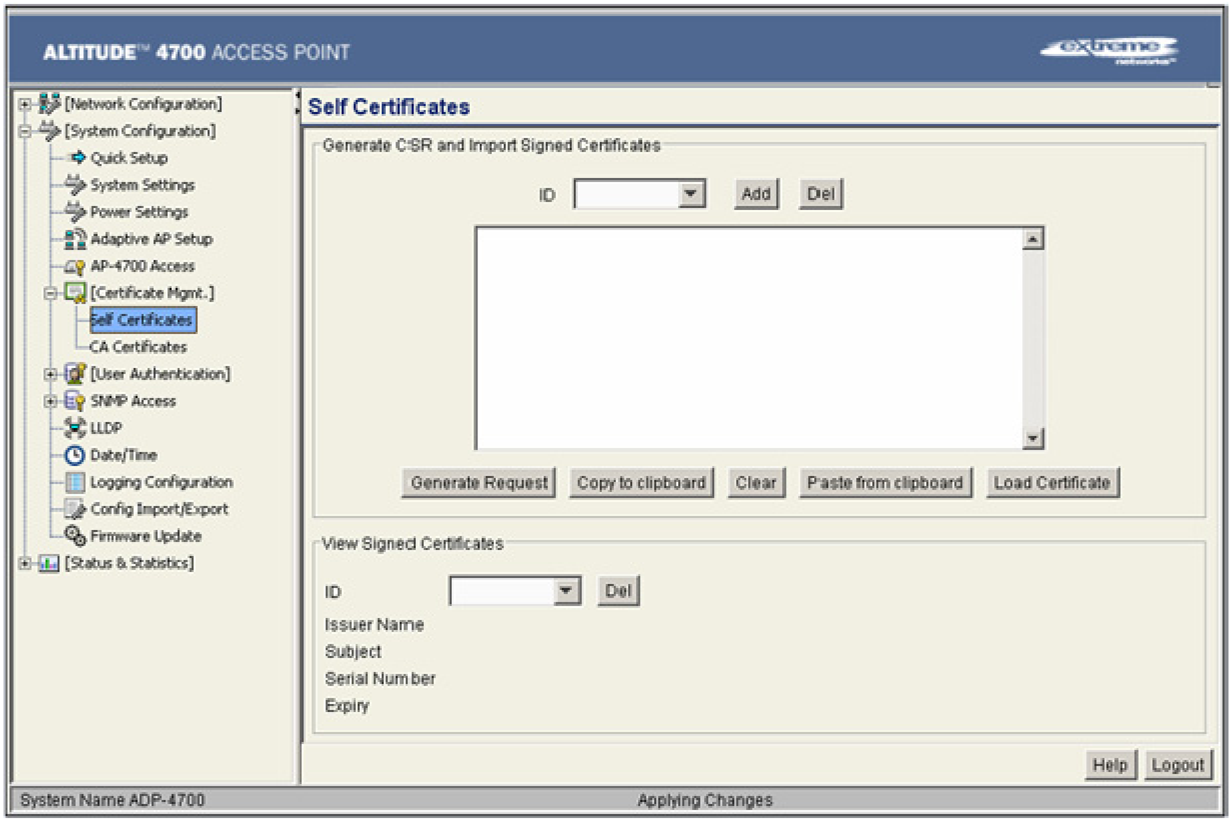
Key Length

Defines the length of the key. Possible values are 512, 1024, and 2048.

4 When the form is completed, click the *Generate* button.

The Certificate Request screen disappears and the ID of the generated certificate request displays in the drop-down list of certificates within the Self Certificates screen.

5 Click the *Generate Request* button.



The generated certificate request displays in Self Certificates screen text box.

6 Click the *Copy to Clipboard* button.

The content of certificate request is copied to the clipboard.

Create an email to your CA, paste the content of the request into the body of the message and send it to the CA.

The CA signs the certificate and will send it back. Once received, copy the content from the email into the clipboard.

7 Click the *Paste from clipboard* button.

The content of the email displays in the window.

Click the *Load Certificate* button to import the certificate and make it available for use as a VPN authentication option. The certificate ID displays in the Signed list.

NOTE

If the access point is restarted after a certificate request has been generated but before the signed certificate is imported, the import will not execute properly. Do not restart the access point during this process.

8 To use the certificate for a VPN tunnel, first define a tunnel and select the IKE settings to use either RSA or DES certificates. For additional information on configuring VPN tunnels, see "Configuring VPN Tunnels" on page 225.

Creating a Certificate for Onboard Radius Authentication

The access point can use its on-board RADIUS Server to generate certificates to authenticate MUs for use with the Access Point. In addition, a Windows 2000 or 2003 Server is used to sign the certificate before downloading it back to the Access Point's on-board RADIUS server and loading the certificate for use with the Access Point.

Both a CA and Self certificate are required for Onboard RADIUS Authentication. For information on CA Certificates, see "Importing a CA Certificate" on page 91. Ensure the certificate is in a Base 64 Encoded format or risk loading an invalid certificate.

CAUTION

If using the RADIUS time-based authentication feature to authenticate Access Point user permissions, ensure the Access Point's time is synchronized with the CA server used to generate certificate requests.

CAUTION

Self certificates can only be generated using the Access Point GUI and CLI interfaces. No functionality exists for creating a self-certificate using the Access Point's SNMP configuration option.

To create a self certificate for on-board RADIUS authentication:

1. Select *System Configuration* > *Certificate Mgmt* > *Self Certificates* from the access point menu tree.
2. Click on the *Add* button to create the certificate request.

   The *Certificate Request* screen displays.
3. Complete the request form with the pertinent information.

   Key ID (required)
   Enter a logical name for the certificate to help distinguish between certificates. The name can be up to 7 characters in length.

   Subject (required)
   The required *Subject* value contains important information about the certificate. Contact the CA signing the certificate to determine the content of the Subject parameter.

   Department
   Optionally enter a value for your organizations's department name if needing to differentiate the certificate from similar certificates used in other departments within your organization.

   Organization
   Optionally enter the name of your organization for supporting information for the certificate request.

   City
   Optionally enter the name of the City where the Access Point (using the certificate) resides.

   State
   Optionally enter the name of the State where the Access Point (using the certificate) resides.

   Postal Code
   Optionally enter the name of the Postal (Zip) Code where the Access Point (using the certificate) resides.

   Country Code
   Optionally enter the Access Point's Country Code.

   Email
   Enter an organizational email address (avoid using a personal address if possible) to associate the request with the proper requesting organization.

Domain Name — Ensure the Domain name is the name of the CA Server. This value must be set correctly to ensure the certificate is properly generated.

IP Address — Enter the IP address of this Access Point (as you are using the Access Point's onboard RADIUS server).

Signature Algorithm — Use the drop-down menu to select the signature algorithm used for the certificate. Options include:

- *MD5-RSA*—Message Digest 5 algorithm in combination with RSA encryption.
- *SHA1-RSA*—Secure Hash Algorithm 1 in combination with RSA encryption.

Key Length — Defines the length of the key. Possible values are 512, 1024, and 2048. Extreme Networks recommends setting this value to 1024 to ensure optimum functionality.

4. Complete as many of the optional values within the *Certificate Request* screen as possible.
5. When the form is completed, click the *Generate* button from within the Certificate Request screen.

   The Certificate Request screen disappears and the ID of the generated certificate request displays in the drop-down list of certificates within the Self Certificates screen.

NOTE

A Warning screen may display at this phase stating key information could be lost if you proceed with the certificate request. Click the OK button to continue, as the certificate has not been signed yet.

6. Click the *Generate Request* button from within the Self Certificates screen. The certificate content displays within the Self Certificate screen.
7. Click the *Copy to clipboard* button. Save the certificate content to a secure location.
8. Connect to the Windows 2000 or 2003 server used to sign the certificate.
9. Select the *Request a certificate* option. Click *Next* to continue.
10. Select the *Advanced request* checkbox from within the Choose Request Type screen and click Next to continue.
11. From within the Advanced Certificate Requests screen, select the *Submit a certificate request using a base 64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS file* option. Click *Next* to continue.
12. Paste the content of certificate in the *Saved Request* field (within the Submit a Saved Request screen).

NOTE

An administrator must make sure the Web Server option is available as a selectable option for those without administrative privileges.

If you do not have administrative privileges, ensure the *Web Server* option has been selected from the Certificate Template drop-down menu. Click Submit.

13. Select the *Base 64 encoded* checkbox option from within the Certificate Issued screen and select the *Download CA Certificate* link.

    A *File Download* screen displays prompting the user to select the download location for the certificate.
14. Click the *Save* button and save the certificate to a secure location.

15 Load the certificates on the Access Point.

CAUTION

Ensure the CA Certificate is loaded before the Self Certificate, or risk an invalid certificate load.

16 Open the certificate file and copy its contents into the CA Certificates screen by clicking the *Paste from Clipboard* button.

The certificate is now ready to be loaded into the Access Point's flash memory.

17 Click the *Import root CA Certificate* button from within the CA Certificates screen.

18 Verify the contents of the certificate file display correctly within the CA Certificates screen.

19 Open the certificate file and copy its contents into the Self Certificates screen by clicking the *Paste from Clipboard* button.

20 Click the *Load Certificate* button.

21 Verify the contents of the certificate file display correctly within the Self Certificates screen.

The certificate for the onboard RADIUS authentication of MUs has now been generated and loaded into the Access Point's flash memory.

Configuring SNMP Settings

Simple Network Management Protocol (SNMP) facilitates the exchange of management information between network devices. SNMP uses *Management Information Bases (MIBs)* to manage the device configuration and monitor Internet devices in potentially remote locations. MIB information accessed via SNMP is defined by a set of managed objects called *object identifiers (OIDs)*. An object identifier (OID) is used to uniquely identify each object variable of a MIB. The Access Point's download site contains the following MIB files supporting the Access Point:

- EXTR-CC-AP4700-MIB-2.0 (standard MIB file)
- EXTR-AP4700-MIB-02a02

NOTE

The EXTR-AP4700-MIB-02a02 contains the majority of the information contained within the EXTR-CC-AP4700-MIB-2.0 file. The remaining portion of the EXTR-AP4700-MIB-02a02 contains supplemental information unique to the Access Point feature set.

Use the table below to locate the MIB where the given feature can be configured.

Feature	MIB	Feature	MIB
LAN Configuration	EXTR-AP4700-MIB-02a02	Subnet Configuration	EXTR-CC-AP4700-MIB-2.0
VLAN Configuration	EXTR-AP4700-MIB-02a02	DHCP Server Configuration	EXTR-CC-AP4700-MIB-2.0
802.1x Port Authentication	EXTR-AP4700-MIB-02a02	Advanced DHCP Server Configuration	EXTR-CC-AP4700-MIB-2.0
Ethernet Type Filter Configuration	EXTR-AP4700-MIB-02a02	WAN IP Configuration	EXTR-CC-AP4700-MIB-2.0

Feature	MIB	Feature	MIB
Wireless Configuration	EXTR-AP4700-MIB-02a02	PPP Over Ethernet	EXTR-CC-AP4700-MIB-2.0
Security Configuration	EXTR-AP4700-MIB-02a02	NAT Address Mapping	EXTR-CC-AP4700-MIB-2.0
MU ACL Configuration	EXTR-AP4700-MIB-02a02	VPN Tunnel Configuration	EXTR-CC-AP4700-MIB-2.0
QOS Configuration	EXTR-AP4700-MIB-02a02	VPN Tunnel status	EXTR-CC-AP4700-MIB-2.0
Radio Configuration	EXTR-AP4700-MIB-02a02	Content Filtering	EXTR-CC-AP4700-MIB-2.0
Rate Limiting	EXTR-AP4700-MIB-02a02	Rogue AP Detection	EXTR-CC-AP4700-MIB-2.0
SNMP Trap Selection	EXTR-AP4700-MIB-02a02	Firewall Configuration	EXTR-CC-AP4700-MIB-2.0
SNMP RF Trap Thresholds	EXTR-AP4700-MIB-02a02	LAN to WAN Access	EXTR-CC-AP4700-MIB-2.0
Config Import/ Export	EXTR-AP4700-MIB-02a02	Advanced LAN Access	EXTR-CC-AP4700-MIB-2.0
MU Authentication Stats	EXTR-AP4700-MIB-02a02	Router Configuration	EXTR-CC-AP4700-MIB-2.0
WNMP Ping Configuration	EXTR-AP4700-MIB-02a02	System Settings	EXTR-CC-AP4700-MIB-2.0
Known AP Stats	EXTR-AP4700-MIB-02a02	AP 5131 Access	EXTR-CC-AP4700-MIB-2.0
Flash LEDs	EXTR-AP4700-MIB-02a02	Certificate Mgt	EXTR-CC-AP4700-MIB-2.0
Automatic Update	EXTR-AP4700-MIB-02a02	SNMP Access Configuration	EXTR-CC-AP4700-MIB-2.0
		SNMP Trap Configuration	EXTR-CC-AP4700-MIB-2.0
		NTP Server Configuration	EXTR-CC-AP4700-MIB-2.0
		Logging Configuration	EXTR-CC-AP4700-MIB-2.0
		Firmware Update	EXTR-CC-AP4700-MIB-2.0
		Wireless Stats	EXTR-CC-AP4700-MIB-2.0
		Radio Stats	EXTR-CC-AP4700-MIB-2.0
		MU Stats	EXTR-CC-AP4700-MIB-2.0
		Automatic Update	EXTR-CC-AP4700-MIB-2.0

SNMP allows a network administrator to manage network performance, find and solve network problems, and plan for network growth. The access point supports SNMP management functions for gathering information from its network components, communicating that information to specified users and configuring the Access Point. All the fields available within the Access Point are also configurable within the MIB.

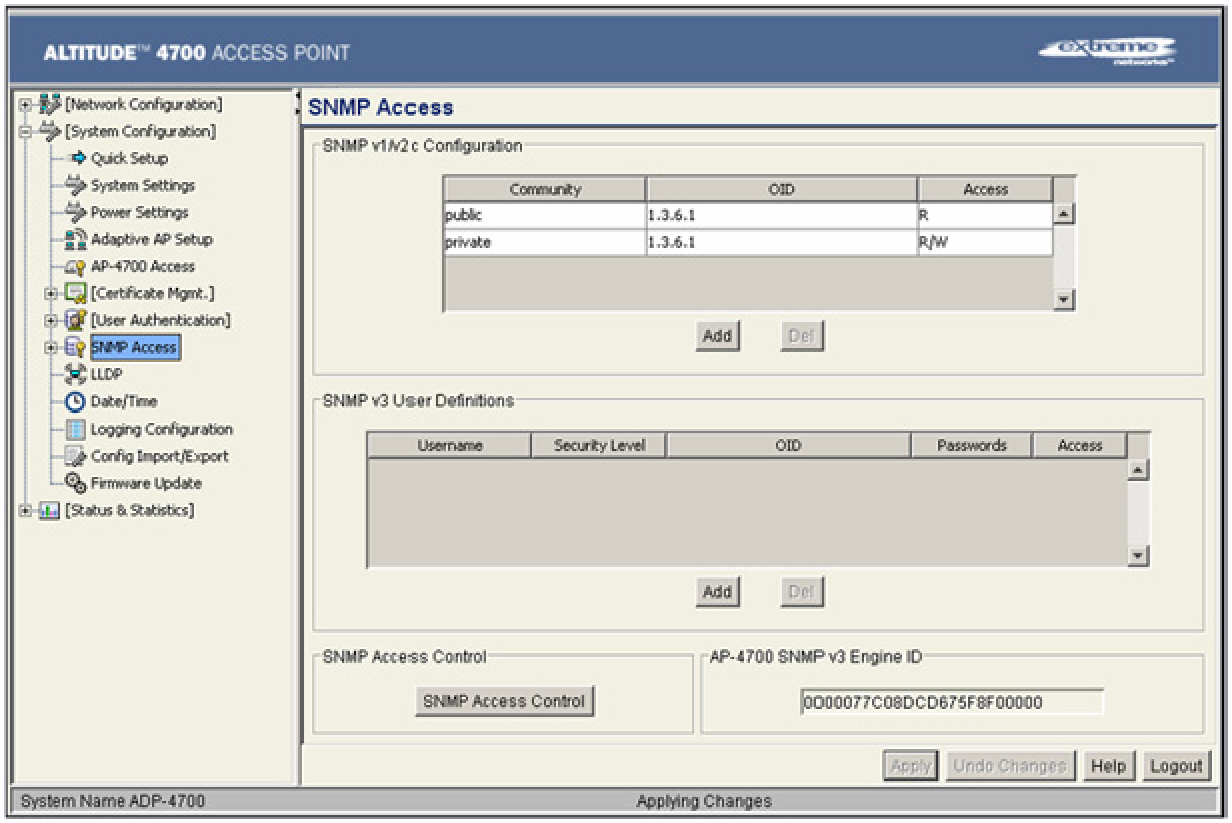
The access point SNMP agent functions as a command responder and is a multilingual agent responding to SNMPv1, v2c and v3 managers (command generators). The factory default configuration maintains SNMPv1/2c support of the community names, hence providing backward compatibility.

SNMP v1/v2c community definitions and SNMP v3 user definitions work independently, and both use the *Access Control List (ACL)* of the *SNMP Access Control* sub-screen.

Use the *SNMP Access* screen to define SNMP v1/v2c community definitions and SNMP v3 user definitions. SNMP version 1 (v1) provides a strong network management system, but its security is relatively weak. The improvements in SNMP version 2c (v2c) do not include the attempted security enhancements of other version-2 protocols. Instead, SNMP v2c defaults to SNMP-standard community strings for read-only and read/write access. SNMP version 3 (v3) further enhances protocol features, providing much improved security. SNMP v3 encrypts transmissions and provides authentication for users generating requests.

To configure SNMP v1/v2c community definitions and SNMP v3 user definitions for the access point:

1 Select *System Configuration* > *SNMP Access* from the access point menu tree.



SNMP Access

SNMP v1/v2c Configuration

Community	OID	Access
public	1.3.6.1	R
private	1.3.6.1	R/W

SNMP v3 User Definitions

Username	Security Level	OID	Passwords	Access

SNMP Access Control

AP-4700 SNMP v3 Engine ID: 0D00077C08DCD675F8F00000

System Name ADP-4700

Applying Changes

SNMP v1/v2c community definitions allow read-only or read/write access to access point management information. The SNMP community includes users whose IP addresses are specified on the *SNMP Access Control* screen.

A read-only community string allows a remote device to retrieve information, while a read/write community string allows a remote device to modify settings. Extreme Networks recommends considering adding a community definition using a site-appropriate name and access level. Set up a read/write definition (at a minimum) to facilitate full access by the access point administrator.

2 Configure the *SNMP v1/v2 Configuration* field (if SNMP v1/v2 is used) to add or delete community definitions, name the community, specify the OID and define community access.

Add — Click *Add* to create a new SNMP v1/v2c community definition.

Delete — Select *Delete* to remove a SNMP v1/v2c community definition.

Community — Use the *Community* field to specify a site-appropriate name for the community. The name is required to match the name used within the remote network management software.

OID

Use the *OID* (Object Identifier) pull-down list to specify a setting of All or a enter a Custom OID. Select *All* to assign the user access to all OIDs in the MIB. The OID field uses numbers expressed in dot notation.

Access

Use the *Access* pull-down list to specify *read-only (R)* access or *read/write (RW)* access for the community. Read-only access allows a remote device to retrieve Access Point information, while read/write access allows a remote device to modify Access Point settings.

3 Configure the *SNMP v3 User Definitions* field (if SNMP v3 is used) to add and configure SNMP v3 user definitions.

SNMP v3 user definitions allow read-only or read/write access to management information as appropriate.

Add

Click *Add* to create a new entry for an SNMP v3 user.

Delete

Select *Delete* to remove an entry for an SNMP v3 user.

Username

Specify a username by typing an alphanumeric string of up to 31 characters.

Security Level

Use the *Security Level* area to specify a security level of *noAuth (no authorization)*, *AuthNoPriv (authorization without privacy)*, or *AuthPriv (authorization with privacy)*.

The *NoAuth* setting specifies no login authorization or encryption for the user.

The *AuthNoPriv* setting requires login authorization, but no encryption.

The *AuthPriv* setting requires login authorization and uses the *Data Encryption Standard (DES)* protocol.

OID

Use the *OID* (Object Identifier) area to specify a setting of All or enter a Custom OID. Select *All* to assign the user access to all OIDs in the MIB. The OID field uses numbers expressed in dot notation.

Passwords

Select *Passwords* to display the *Password Settings* screen for specifying authentication and password settings for an SNMP v3 user. The maximum password length is 11 characters. Use the *Authentication Algorithm* drop-down menu to specify *MD5* or *SHA1* as the authentication algorithm. Use the Privacy Algorithm drop-down menu to define an algorithm of *DES* or *AES-128bit*.

When entering the same username on the *SNMP Traps* and *SNMP Access* screens, the password entered on the SNMP Traps page overwrites the password entered on the SNMP Access page. To avoid this problem, enter the same password on both pages.

Access

Use the *Access* pull-down list to specify *read-only (R)* access or *read/write (RW)* access for a user. Read-only access permits a user to retrieve access point information, while read/write access allows a user to modify access pointsettings.

4 Specify the users who can read and optionally modify the SNMP-capable client.

SNMP Access Control

Click the *SNMP Access Control* button to display the *SNMP Access Control* screen for specifying which users can read SNMP-generated information and potentially modify related settings from an SNMP-capable client.

The SNMP Access Control screen's *Access Control List* (ACL) uses Internet Protocol (IP) addresses to restrict access to the AP's SNMP interface. The ACL applies to both SNMP v3 user definitions and SNMP v1/v2c community definitions.

For detailed instructions of configuring SNMP user access and modification privileges, see "Configuring SNMP Access Control" on page 101.

5 If configuring SNMP v3 user definitions, set the SNMP v3 engine ID.

SNMP v3 Engine ID

The access point *SNMP v3 Engine ID* field lists the unique SNMP v3 Engine ID for the access point. This ID is used in SNMP v3 as the source for a trap, response or report. It is also used as the destination ID when sending *get, getnext*, *getbulk*, *set* or *inform* commands.

6 Click *Apply* to save any changes to the SNMP Access screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

7 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the SNMP Access screen to the last saved configuration.

8 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

For additional SNMP configuration information, see:

- Configuring SNMP Access Control on page 101
- Enabling SNMP Traps on page 103
- Configuring Specific SNMP Traps on page 105
- Configuring SNMP RF Trap Thresholds on page 107

Configuring SNMP Access Control

Use the *SNMP Access Control* screen (as launched from the SNMP Access screen) to specify which users can read SNMP generated information and, if capable, modify related settings from an SNMP-capable client.

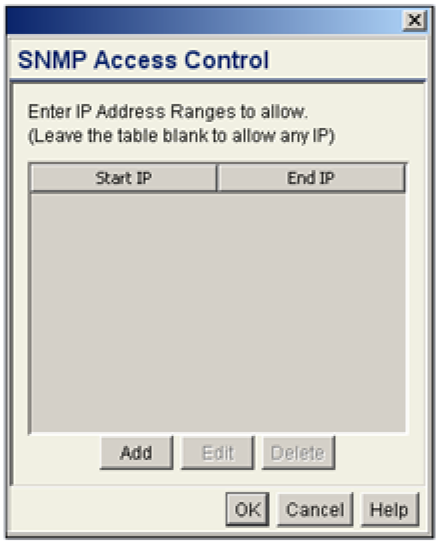
Use the SNMP Access Control screen's *Access Control List (ACL)* to limit, by Internet Protocol (IP) address, who can access the access point SNMP interface.

NOTE

The ACL applies to both SNMP v3 user definitions and SNMP v1/v2c community definitions on the access point SNMP Access screen.

To configure SNMP user access control for the access point:

1 Select *System Configuration > SNMP Access* from the access point menu tree. Click on the *SNMP Access Control* button from within the SNMP Access screen.



SNMP Access Control

Enter IP Address Ranges to allow.
(Leave the table blank to allow any IP)

Start IP	End IP

2 Configure the SNMP Access Control screen to add the IP addresses of those users receiving SNMP access.

Access Control List
Enter Start IP and End IP addresses (numerical addresses only, no DNS names supported) to specify a range of user that can access the access point SNMP interface. An SNMP-capable client can be set up whereby only the administrator (for example) can use a read/write community definition.

Use just the Starting IP Address column to specify a single SNMP user. Use both the Starting IP Address and Ending IP Address columns to specify a range of addresses for SNMP users.

To add a single IP address to the ACL, enter the same IP address in the Start IP and End IP fields.

Leave the ACL blank to allow access to the SNMP interface from the IP addresses of all authorized users.

Add
Click *Add* to create a new ACL entry.

Edit
Click *Edit* to revise an existing ACL entry.

Delete
Click *Delete* to remove a selected ACL entry for one or more SNMP users.

OK
Click *Ok* to return to the SNMP Access screen. Click *Apply* within the SNMP Access screen to save any changes made on the SNMP Access Control screen.

Cancel
Click *Cancel* to undo any changes made on the SNMP Access Control screen. This reverts all settings for this screen to the last saved configuration.

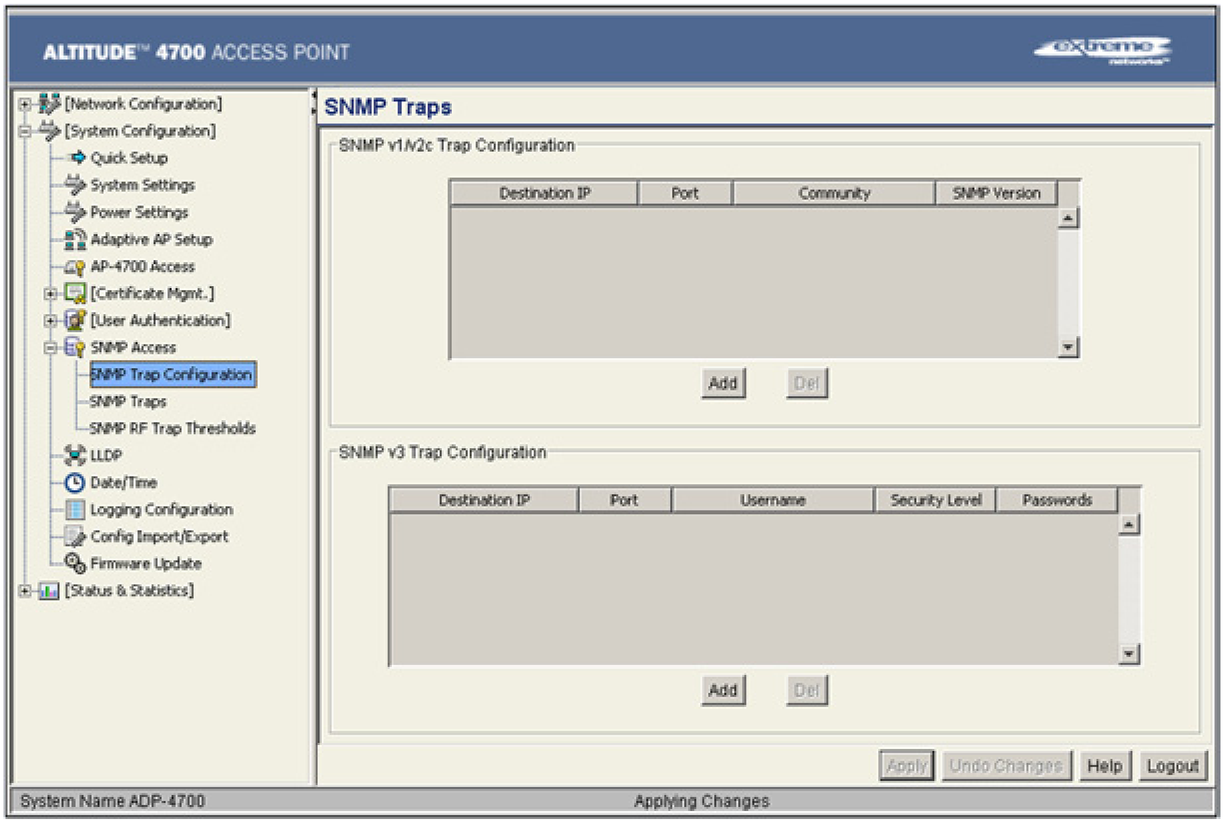
Enabling SNMP Traps

SNMP provides the ability to send traps to notify the administrator that trap conditions are met. Traps are network packets containing data relating to network devices, or SNMP agents, that send the traps. SNMP management applications can receive and interpret these packets, and optionally can perform responsive actions. SNMP trap generation is programmable on a trap-by-trap basis.

Use the *SNMP Traps Configuration* screen to enable traps and to configure appropriate settings for reporting this information. Trap configuration depends on the network machine that receives the generated traps. SNMP v1/v2c and v3 trap configurations function independently. In a mixed SNMP environment, generated traps can be sent using configurations for both SNMP v1/v2c and v3.

To configure SNMP traps on the access point:

1 Select *System Configuration* > *SNMP Access* > *SNMP Trap Configuration* from the access point menu tree.



2 Configure the *SNMP v1/v2c Trap Configuration* field (if SNMP v1/v2c Traps are used) to modify the following:

Add — Click *Add* to create a new SNMP v1/v2c Trap Configuration entry.

Delete — Click *Delete* to remove a selected SNMP v1/v2c Trap Configuration entry.

Destination IP — Specify a numerical (non DNS name) destination IP address for receiving the traps sent by the access point SNMP agent.

Add

Click *Add* to create a new SNMP v1/v2c Trap Configuration entry.

Port

Specify a destination *User Datagram Protocol (UDP)* port for receiving traps. The default is 162.

Community

Enter a community name specific to the SNMP-capable client that receives the traps.

SNMP Version

Use the SNMP Version drop-down menu to specify v1 or v2.

Some SNMP clients support only SNMP v1 traps, while others support SNMP v2 traps and possibly both, verify the correct traps are in use with clients that support them.

3 Configure the *SNMP v3 Trap Configuration* field (if SNMP v3 Traps are used) to modify the following:

Add

Click *Add* to create a new SNMP v3 Trap Configuration entry.

Delete

Select *Delete* to remove an entry for an SNMP v3 user.

Destination IP

Specify a numerical (non DNS name) destination IP address for receiving the traps sent by the access point SNMP agent.

Port

Specify a destination *User Datagram Protocol (UDP)* port for receiving traps.

Username

Enter a username specific to the SNMP-capable client receiving the traps.

Security Level

Use the *Security Level* drop-down menu to specify a security level of *noAuth* (no authorization), *AuthNoPriv* (authorization without privacy), or *AuthPriv* (authorization with privacy).

The “NoAuth” setting specifies no login authorization or encryption for the user. The “AuthNoPriv” setting requires login authorization, but no encryption. The “AuthPriv” setting requires login authorization and uses the *Data Encryption Standard (DES)*.

Passwords

Select *Passwords* to display the *Password Settings* screen for specifying authentication and password settings for an SNMP v3 user. The maximum password length is 11 characters. Use the *Authentication Algorithm* drop-down menu to specify *MD5* or *SHA1* as the authentication algorithm. Use the Privacy Algorithm drop-down menu to define an algorithm of *DES* or *AES-128bit*.

If entering the same username on the SNMP Traps and SNMP Access screens, the password entered on the SNMP Traps page overwrites the password entered on the SNMP Access page. To avoid this problem, enter the same password on both pages.

4 Click *Apply* to save any changes to the SNMP Trap Configuration screen. Navigating away from the screen without clicking the Apply button results in all changes being lost.

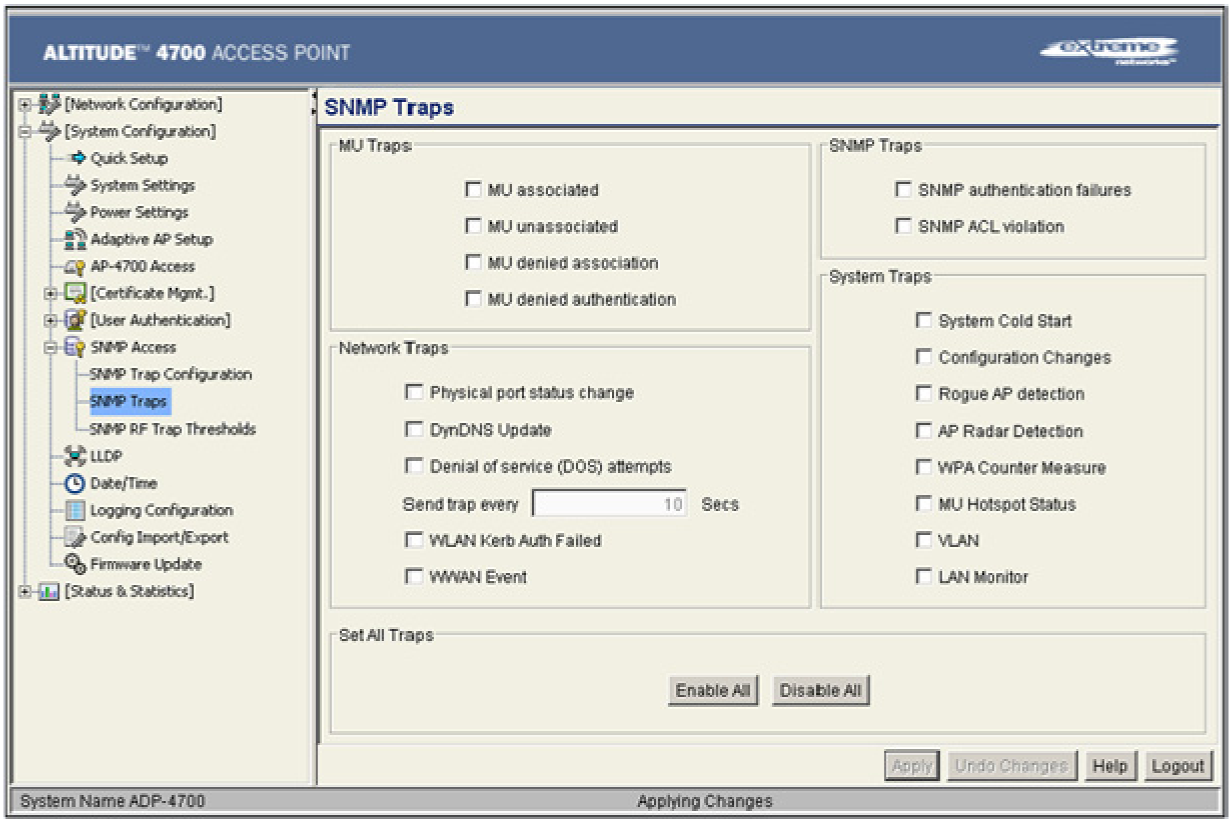
5 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on SNMP Trap Configuration screen to the last saved configuration.

6 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring Specific SNMP Traps

Use the *SNMP Traps* screen to enable specific traps on the access point. Extreme Networks recommends defining traps to capture unauthorized devices operating within the access point coverage area. Trap configuration depends on the network machine that receives the generated traps. SNMP v1/v2c and v3 trap configurations function independently. In a mixed SNMP environment, traps can be sent using configurations for both SNMP v1/v2c and v3. To configure specific SNMP traps on the access point:

1 Select *System Configuration* > *SNMP Access* > *SNMP Traps* from the menu tree.



SNMP Traps

MU Traps

□ MU associated

□ MU unassociated

□ MU denied association

□ MU denied authentication

Network Traps

□ Physical port status change

□ DynDNS Update

□ Denial of service (DOS) attempts

Send trap every 10 Secs

□ WLAN Kerb Auth Failed

□ WWAN Event

SNMP Traps

□ SNMP authentication failures

□ SNMP ACL violation

System Traps

□ System Cold Start

□ Configuration Changes

□ Rogue AP detection

□ AP Radar Detection

□ WPA Counter Measure

□ MU Hotspot Status

□ VLAN

□ LAN Monitor

Set All Traps

System Name ADP-4700

Applying Changes

2 Configure the *MU Traps* field to generate traps for MU associations, MU association denials and MU authentication denials. When a trap is enabled, a trap is sent every 10 seconds until the condition no longer exists.

MU associated
Generates a trap when an MU becomes associated with one of the access point's WLANs.

MU unassociated
Generates a trap when an MU becomes unassociated with (or gets dropped from) one of the access point's WLANs.

MU denied association
Generates a trap when an MU is denied association to a access point WLAN. Can be caused when the maximum number of MUs for a WLAN is exceeded or when an MU violates the access point's *Access Control List (ACL).*

MU denied authentication
Generates a trap when an MU is denied authentication on one of the AP's WLANs. Can be caused by the MU being set for the wrong authentication type for the WLAN or by an incorrect key or password.

3 Configure the *SNMP Traps* field to generate traps when SNMP capable MUs are denied authentication privileges or are subject of an ACL violation. When a trap is enabled, a trap is sent every 5 seconds until the condition no longer exists.

SNMP authentication failures
Generates a trap when an SNMP-capable client is denied access to the access point's SNMP management functions or data. This can result from an incorrect login, or missing/incorrect user credentials.

SNMP ACL violation
Generates a trap when an SNMP client cannot access SNMP management functions or data due to an Access Control List (ACL) violation. This can result from a missing/incorrect IP address entered within the *SNMP Access Control* screen.

4 Configure the *Network Traps* field to generate traps when the access point's link status changes or when the AP's firewall detects a DOS attack.

Physical port status change
Generates a trap whenever the status changes on the access point. The physical port status changes when a link is lost between the access point and a connected device.

DynDNS Update
Generates a trap whenever domain name information is updated as a result of the IP address associated with that domain being modified.

Denial of service (DOS) attempts
Generates a trap whenever a *Denial of Service (DOS)* attack is detected by the access point firewall. A new trap is sent at the specified interval until the attack has stopped.

Send trap every
Defines the interval in seconds the access point uses to generate a trap until the Denial of Service attack is stopped. Default is 10 seconds.

WLAN Kerb Auth Failed
Generates a trap when the Access Point detects a WLAN Kerberos authorization failure.

WWAN Event
Generates a trap when the Access Point detects the presence of a 3G WWAN card, the Access Point establishes (or fails to establish) a 3G WWAN connection, or the Access Point detects a 3G WWAN card disconnection, removal or resumed connection.

5 Configure the *System Traps* field to generate traps when the access point re-initializes during transmission, saves its configuration file. When a trap is enabled, a trap is sent every 5 seconds until the condition no longer exists.

System Cold Start
Generates a trap when the access point re-initializes while transmitting, possibly altering the SNMP agent's configuration or protocol entity implementation.

Configuration Changes
Generates a trap whenever changes to the access point's configuration file are saved.

Rogue AP Detection
Generates a trap if a Rogue AP is detected by the access point.

AP Radar Detection
Generates a trap if an AP is detected using a form of radar detection.

WPA Counter Measure
Generates a trap if an attack is detected against the WPA Key Exchange Mechanism.

MU Hotspot Status
Generates a trap when a change to the status of MU hotspot member is detected.

System Cold Start	Generates a trap when the access point re-initializes while transmitting, possibly altering the SNMP agent's configuration or protocol entity implementation.
VLAN	Generates a trap when a change to a VLAN state is detected.
LAN Monitor	Generates a trap when a change to the LAN monitoring state is detected.

6 Click *Apply* to save any changes to the SNMP Traps screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

7 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on SNMP Traps screen to the last saved configuration.

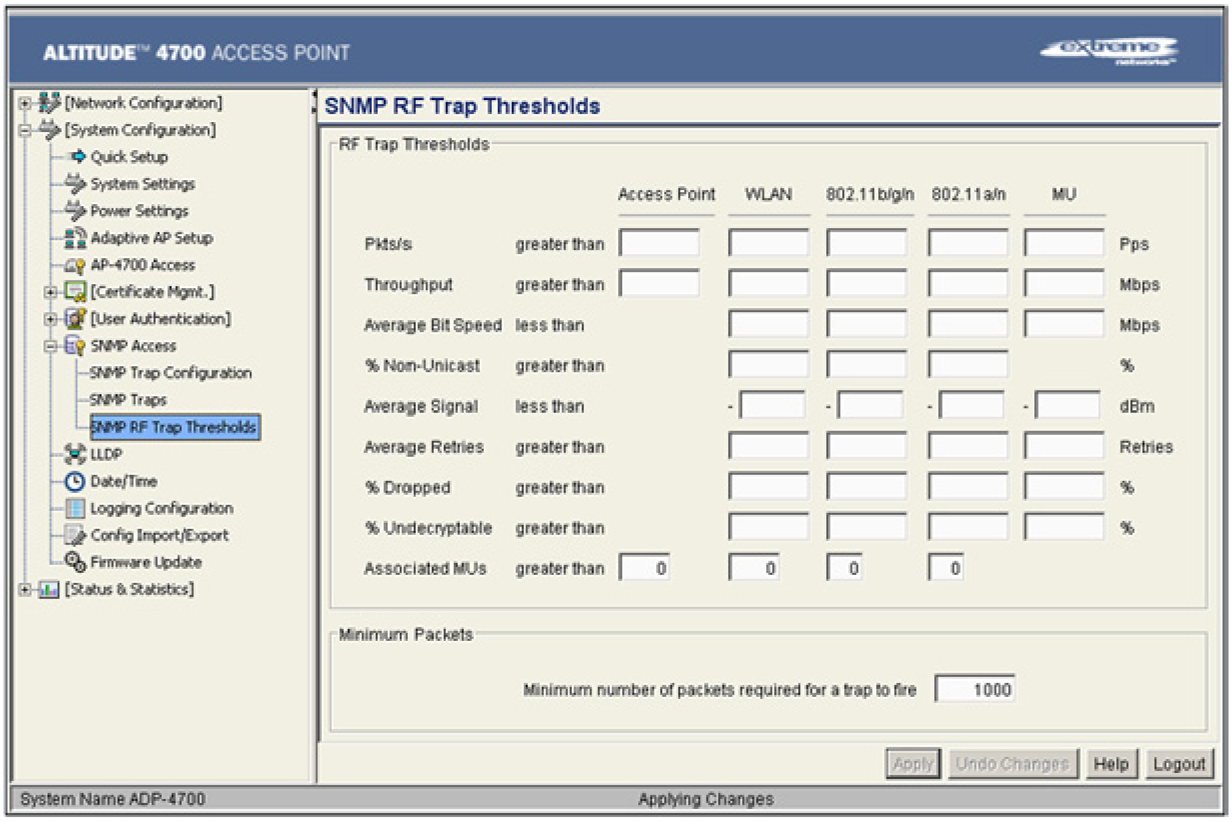
8 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring SNMP RF Trap Thresholds

Use the *SNMP RF Trap Threshold* screen as a means to track RF activity and the access point's radio and associated MU performance. SNMP RF Traps are sent when RF traffic exceeds defined limits set in the *RF Trap Thresholds* field of the SNMP RF Traps screen. Thresholds are displayed for the access point, WLAN, selected radio and the associated MU.

To configure specific SNMP RF Traps on the access point:

1 Select *System Configuration* > *SNMP Access* > *SNMP RF Trap Thresholds* from the menu tree.



SNMP RF Trap Thresholds

RF Trap Thresholds

		Access Point	WLAN	802.11b/g/n	802.11a/n	MU	
Pkts/s	greater than						Pps
Throughput	greater than						Mbps
Average Bit Speed	less than						Mbps
% Non-Unicast	greater than						%
Average Signal	less than		-	-	-	-	dBm
Average Retries	greater than						Retries
% Dropped	greater than						%
% Undecryptable	greater than						%
Associated MUs	greater than	0	0	0	0		

Minimum Packets

Minimum number of packets required for a trap to fire 1000

System Name ADP-4700 Applying Changes

2 Configure the *RF Trap Thresholds* field to define device threshold values for SNMP traps.

NOTE

Average Bit Speed,% of Non-Unicast, Average Signal, Average Retries,% Dropped and % Undecryptable are not Access Point statistics.

Pkts/s
Enter a maximum threshold for the total throughput in Pps (Packets per second).

Throughput
Set a maximum threshold for the total throughput in Mbps (Megabits per second).

Average Bit Speed
Enter a minimum threshold for the average bit speed in Mbps (Megabits per second).

Average Signal
Enter a minimum threshold for the average signal strength in dBm for each device.

Average Retries
Set a maximum threshold for the average number of retries for each device.

% Dropped
Enter a maximum threshold for the total percentage of packets dropped for each device. Dropped packets can be caused by poor RF signal or interference on the channel.

% Undecryptable
Define a maximum threshold for the total percentage of packets undecryptable for each device. Undecryptable packets can be the result of corrupt packets, bad CRC checks or incomplete packets.

Associated MUs
Set a maximum threshold for the total number of MUs associated with each device.

3 Configure the *Minimum Packets* field to define a minimum packet throughput value for trap generation.

Minimum number of packets required for a trap to fire
Enter the minimum number of packets that must pass through the device before an SNMP rate trap is sent. Extreme Networks recommends using the default setting of 1000 as a minimum setting for the field.

4 Click *Apply* to save any changes to the SNMP RF Traps screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

5 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on SNMP RF Traps screen to the last saved configuration.

6 Click *Logout* to securely exit the access point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring LLDP Settings

LLDP is a Layer 2 protocol (IEEE standard 802.1AB) used to determine the capabilities of devices such as repeaters, bridges, Access Points, routers and wireless clients. LLDP enables devices to advertise their capabilities and media-specific configurations.

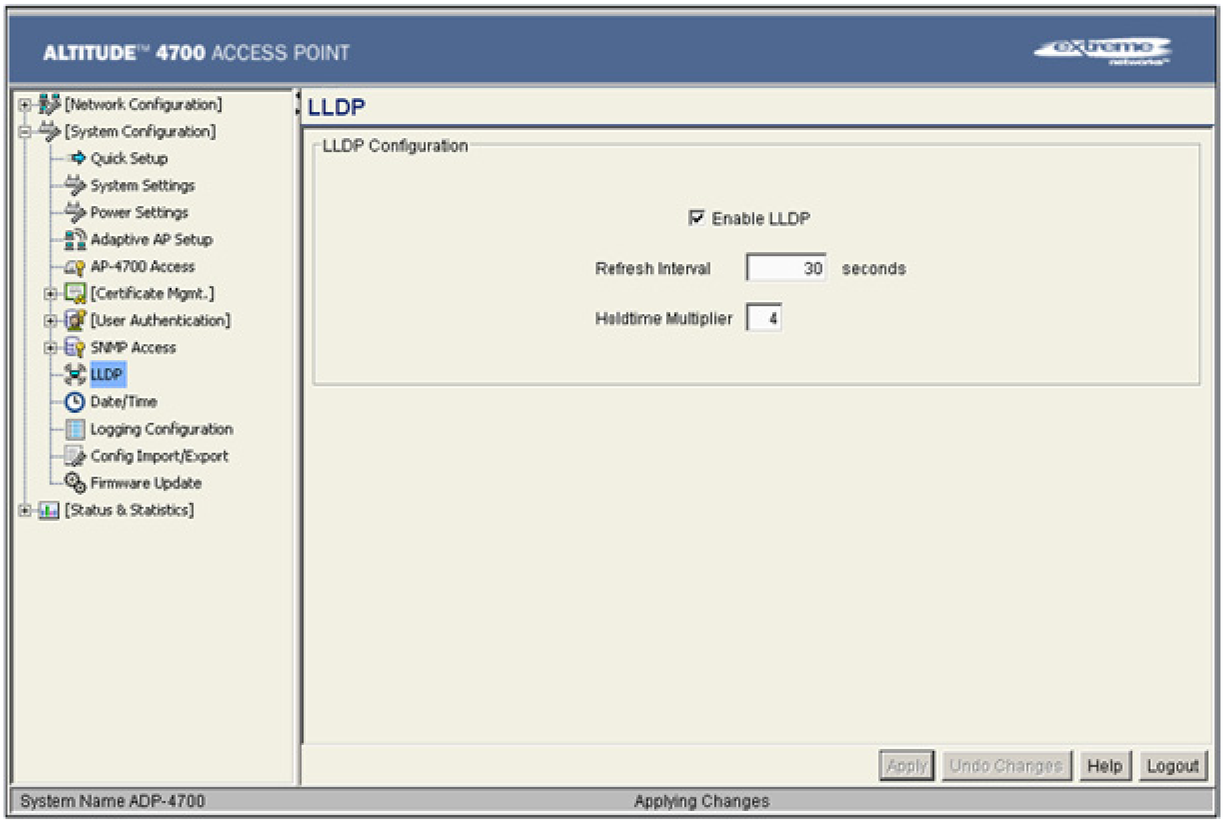
LLDP provides a method of discovering and representing the physical network connections of a given network management domain. The LLDP neighbor discovery protocol allows you to discover and maintain accurate network topologies in a multivendor environment.

The information is in a *Type Length Value* (TLV) format for each data item. TLV information is transmitted in an *LLDP protocol data unit* (LLDPDU), enclosed in an Ethernet frame and sent to a destination MAC address. Certain TLVs are mandatory, and always sent once LLDP is enabled, while other TLVs are optionally configured. LLDP defines a set of common advertisement messages, a protocol for transmitting the advertisements and a method for storing information in received advertisements. A controller can receive and record the TLVs, but not transmit them. The information distributed using LLDP is stored by its recipients in a standard MIB, making it possible for the information to be accessed by an NMS using a management protocol such as SNMP.

LLDP transmits periodic advertisements containing device information and media-specific configuration information to neighbors attached to the same network. LLDP agents cannot solicit information from other agents by way of LLDP.

To configure LLDP support:

1 Select *System Configuration* > *LLDP* from the menu tree.



LLDP

LLDP Configuration

☑ Enable LLDP

Refresh Interval 30 seconds

Holdtime Multiplier 4

System Name ADP-4700

Applying Changes

2 Select the *Enable LLDP* radio button to Enable or Disable the transmission of LLDP advertisements. LLDP is enabled by default.

3 Set a *Refresh Interval* (in seconds 5-32768) to define the refresh-interval/transmit-interval. The Refresh Interval is the interval LLDP frames is transmitted on behalf of the LLDP agent. The default is 30 seconds.

4 Set a *Holdtime Multiplier* (2-10) to define the holdtime multiplier. The default setting is 4.

5 Click *Apply* to save any changes to the LLDP screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

6 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on LLDP screen to the last saved configuration.

7 Click *Logout* to securely exit the access point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring Network Time Protocol (NTP)

Network Time Protocol (NTP) manages time and/or network clock synchronization in the access point-managed network environment. NTP is a client/server implementation. The access point (an NTP client) periodically synchronizes its clock with a master clock (an NTP server). For example, the access point resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

Time synchronization is recommended for the Access Point's network operations. For sites using Kerberos authentication, time synchronization is required. Use the *Date and Time Settings* screen to enable NTP and specify the IP addresses and ports of available NTP servers.

NOTE

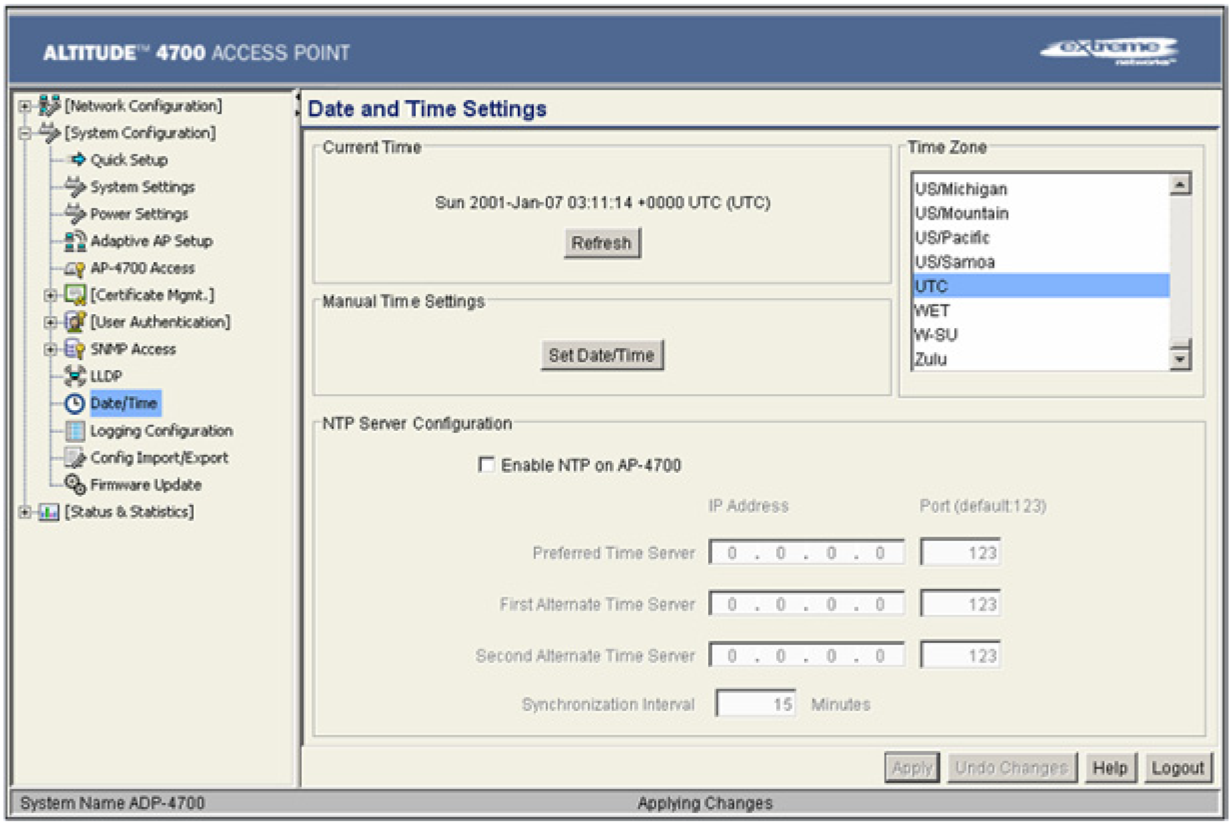
The current time is not set accurately when initially connecting to the access point. Until a server is defined to provide the access point the correct time, or the correct time is manually set, the access point displays 1970-01-01 00:00:00 as the default time.

CAUTION

If using the RADIUS time-based authentication feature to authenticate Access Point user permissions, ensure UTC has been selected from the Date and Time Settings screen's Time Zone field. If UTC is not selected, time based authentication will not work properly. For information on configuring RADIUS time-based authentication, see "Defining User Access Permissions by Group" on page 259.

To manage clock synchronization on the access point:

1 Select *System Configuration* > *Date/Time* from the access point menu tree.



Date and Time Settings

Current Time

Sun 2001-Jan-07 03:11:14 +0000 UTC (UTC)

Manual Time Settings

Time Zone: US/Michigan, US/Mountain, US/Pacific, US/Samoa, UTC, WET, W-SU, Zulu

NTP Server Configuration

□ Enable NTP on AP-4700

	IP Address	Port (default:123)
Preferred Time Server	0 . 0 . 0 . 0	123
First Alternate Time Server	0 . 0 . 0 . 0	123
Second Alternate Time Server	0 . 0 . 0 . 0	123

Synchronization Interval 15 Minutes

System Name ADP-4700 Applying Changes

2 From within the *Current Time* field, click the *Refresh* button to update the time since the screen was displayed by the user.

The Current Time field displays the current time based on the access point system clock. If NTP is disabled or if there are no servers available, the system time displays the access point uptime starting at 1970-01-01 00:00:00, with the time and date advancing.

3 Select the *Set Date/Time* button to display the *Manual Date/Time Setting* screen.

This screen enables the user to manually enter the Access Point's system time using a Year-Month-Day HH:MM:SS format.

This option is disabled when the Enable NTP checkbox has been selected, and therefore should be viewed as a second means to define the Access Point system time.

4 If using the Manual Date/Time Setting screen to define the Access Point's system time, refer to the *Time Zone* field to select the time used to use as complimentary information to the information entered within the Manual Date/Time Setting screen.

CAUTION

If using the RADIUS time-based authentication feature to authenticate Access Point user permissions, ensure UTC has been selected from the Time Zone field. If UTC is not selected, time based authentication will not work properly. For information on configuring RADIUS time-based authentication, see "Defining User Access Permissions by Group" on page 259.

5 If using an NTP server to supply system time to the Access Point, configure the *NTP Server Configuration* field to define the server network address information required to acquire the access point network time.

Enable NTP on AP4700
: Select the *Enable NTP on* access point checkbox to allow a connection between the access point and one or more specified NTP servers. A preferred, first alternate and second alternate NTP server cannot be defined unless this checkbox is selected.

Disable this option (uncheck the checkbox) if Kerberos is not in use and time synchronization is not necessary. This option is disabled by default.

Preferred Time Server
: Specify the numerical (non DNS name) IP address and port of the primary NTP server. The default port is 123.

First Alternate Time Server
: Optionally, specify the numerical (non DNS name) IP address and port of an alternative NTP server to use for time synchronization if the primary NTP server goes down.

Second Alternate Time Server
: Optionally, specify the numerical (non DNS name) and port of yet another NTP server for the greatest assurance of uninterrupted time synchronization.

Synchronization Interval
: Define an interval in minutes the access point uses to synchronize its system time with the NTP server. A synchronization interval value from 15 minutes to 65535 minutes can be specified. For implementations using Kerberos, a synchronization interval of 15 minutes (default interval) or sooner is recommended.

6 Click *Apply* to save any changes to the Date and time Settings screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

7 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on Date and Time Settings screen to the last saved configuration.

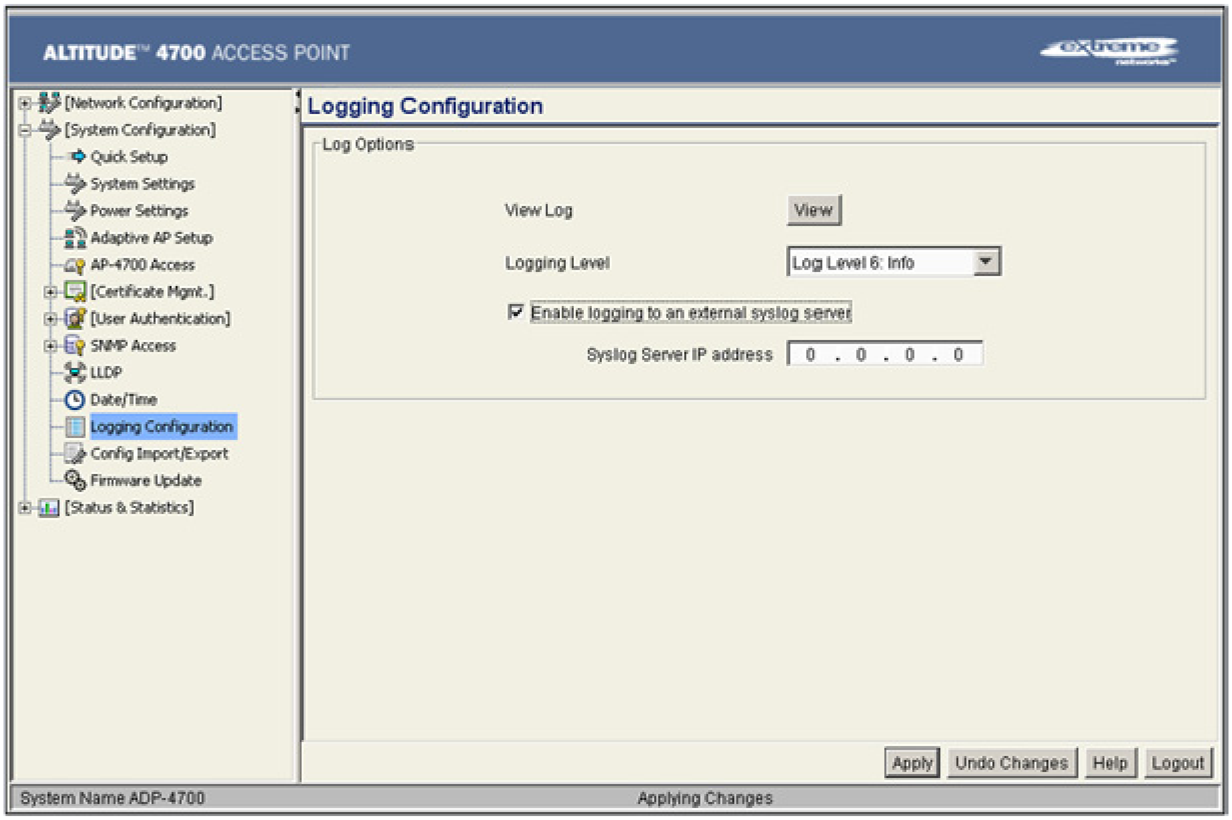
8 Click *Logout* to securely exit the access point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Logging Configuration

The access point provides the capability for periodically logging system events that prove useful in assessing the throughput and performance of the access point or troubleshooting problems on the access point managed *Local Area Network (LAN)*. Use the *Logging Configuration* screen to set the desired logging level (standard syslog levels) and view or save the current access point system log.

To configure event logging for the access point:

1 Select *System Configuration* > *Logging Configuration* from the access point menu tree.



Logging Configuration

Log Options

View Log

Logging Level: Log Level 6: Info

☑ Enable logging to an external syslog server

Syslog Server IP address: 0 . 0 . 0 . 0

System Name ADP-4700

Applying Changes

2 Configure the *Log Options* field to save event logs, set the log level and optionally port the access point's log to an external server.

View Log

Click *View* to save a log of events retained on the access point. The system displays a prompt requesting the administrator password before saving the log. After the password has been entered, click *Get File* to display a dialogue with buttons to *Open* or *Save* the log.txt file. Click Save and specify a location to save the log file.

Use the WordPad application to view the saved log.txt file on a Microsoft Windows based computer. Do not view the log file using Notepad, as the Notepad application does not properly display the formatting of the access point log file. Log entries are not saved in the access point. While the AP is in operation, log data temporarily resides in memory. AP memory is completely cleared each time the AP reboots.

Logging Level	Use the *Logging Level* drop-down menu to select the desired log level for tracking system events. Eight logging levels, (0 to 7) are available. *Log Level 6: Info* is the access point default log level. These are the standard UNIX/LINUX syslog levels.The levels are as follows: 0 - Emergency 1 - Alert 2 - Critical 3 - Errors 4 - Warning 5 - Notice 6 - Info 7 - Debug
Enable logging to an external syslog server	The access point can log events to an external syslog (system log) server. Select the *Enable logging to an external syslog server* checkbox to enable the server to listen for incoming syslog messages and decode the messages into a log for viewing.
Syslog server IP address	If the *Enable logging to an external syslog server* checkbox is selected, the numerical (non DNS name) IP address of an external syslog server is required in order to route the syslog events to that destination.

3 Click *Apply* to save any changes to the Logging Configuration screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

4 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Logging Configuration screen to the last saved configuration.

5 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Importing/Exporting Configurations

All of the configuration settings for an access point can be obtained from another access point in the form of a text file. Additionally, all of the access point's settings can be downloaded to another access point. Use the file-based configuration feature to speed up the setup process significantly at sites using multiple access points.

Another benefit is the opportunity to save the current AP configuration before making significant changes or restoring the default configuration. All options on the Access Point are deleted and updated by the imported file. Therefore, the imported configuration is not a merge with the configuration of the target Access Point. The exported file can be edited with any document editor if necessary.

NOTE

Use the System Settings screen as necessary to restore an access point's default configuration. For more information on restoring configurations, see "Configuring System Settings" on page 78.

NOTE

For configuration file creation and export operations, only the set radio-config (1-8, depending on the SKU) shall be supported.

The export function will always export the encrypted Admin User password. The import function will import the Admin Password only if the Access Point is set to factory default. If the Access Point is not configured to factory default settings, the Admin User password WILL NOT get imported.

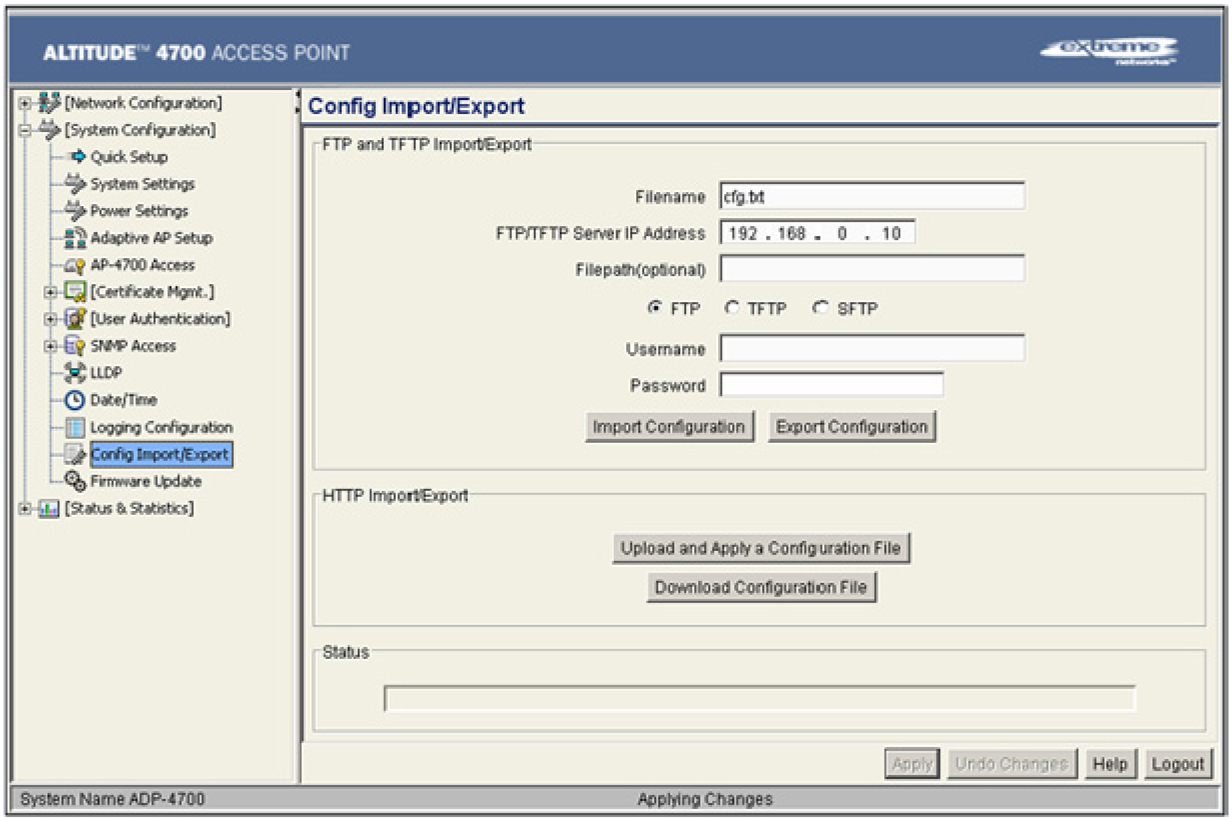
NOTE

When modifying the text file manually and spaces are used for wireless, security, MU policy names etc., ensure you use “\20” between the spaces. For example, “Second\20Floor\20Lab”. When imported, the name would display as “Second Floor Lab”.

Use the *Config Import/Export* screen to configure an import or export operation for access point configuration settings.

To create an importable/exportable access point configuration file:

1 Select *System Configuration* > *Config Import/Export* from the access point menu tree.



Filename: cfg.txt

FTP/TFTP Server IP Address: 192 . 168 . 0 . 10

Filepath(optional):

● FTP ○ TFTP ○ SFTP

Username:

Password:

2 Configure the *FTP and TFTP Import/Export* field to import/export configuration settings.

Filename — Specify the name of the configuration file to be written to the server.

SFTP/FTP/TFTP Server IP
Enter the numerical (non DNS name) IP address of the destination SFTP, FTP or TFTP server where the configuration file is imported or exported.

Filepath (optional)
Defines the optional path name used to import/export the target configuration file.

FTP
Select the FTP radio button if using an FTP server to import or export the configuration.

TFTP
Select the TFTP radio button if using an FTP server to import or export the configuration.

SFTP
Select the SFTP radio button if using a SFTP server to import or export the configuration.

Username
Specify a username to be used when logging in to the FTP server. A username is not required for TFTP server logins.

Password
Define a password allowing access to the server for the import or export operation.

Import Configuration
Click the *Import Configuration* button to import the configuration file from the server with the assigned filename and login information. The system displays a confirmation window indicating the administrator must log out of the access point after the operation completes for the changes to take effect. Click *Yes* to continue the operation. Click *No* to cancel the configuration file import.

Export Configuration
Click the *Export Configuration* button to export the configuration file from the server with the assigned filename and login information. If the IP mode is set to DHCP Client, IP address information is not exported (true for both LAN1, LAN2 and the WAN port). For LAN1 and LAN2, IP address information is only exported when the IP mode is set to either static or DHCP Server. For the WAN port, IP address information is only exported when the *This interface is a DHCP Client* checkbox is not selected.

The system displays a confirmation window prompting the administrator to log out of the access point after the operation completes for the changes to take effect. Click *Yes* to continue the operation. Click *No* to cancel the configuration file export.

3 Configure the *HTTP Import/Export* field to import/export access point configuration settings using HTTP.

CAUTION

For HTTP downloads (exports) to be successful, pop-up messages must be disabled.

Upload and Apply A Configuration File
Click the *Upload and Apply A Configuration File* button to upload a configuration file to this Access Point using HTTP.

Download Configuration File
Click the *Download Configuration File* button to download this Access Point’s configuration file using HTTP.

4 Refer to the *Status* field to assess the completion of the import/export operation.

Status	After executing an operation (by clicking any of the buttons in the window), check the Status field for a progress indicator and messages about the success or errors in executing the Import/Export operation. Possible status messages include: ambiguous input before marker: line <*number* > unknown input before marker: line <*number*> ignored input after marker: line <*number*> additional input required after marker: line <*number*> invalid input length: line <*number*> error reading input: line <*number*> import file from incompatible hardware type: line <*number*> [0] Import operation done [1] Export operation done [2] Import operation failed [3] Export operation failed [4] File transfer in progress [5] File transfer failed [6] File transfer done Auto cfg update: Error in applying config Auto cfg update: Error in getting config file Auto cfg update: Aborting due to fw update failure The <*number*> value appearing at the end of some messages relates to the line of the configuration file where an error or ambiguous input was detected.

CAUTION

If errors occur when importing the configuration file, a parsing message displays defining the line number where the error occurred. The configuration is still imported, except for the error. Consequently, it is possible to import an invalid configuration. The user is required to fix the problem and repeat the import operation until an error-free import takes place.

NOTE

Extreme Networks recommends importing configuration files using the CLI. If errors occur during the import process, they display all at once and are easier to troubleshoot. The Access Point GUI displays errors one at a time, and troubleshooting can be a more time-consuming process.

NOTE

When importing the configuration, a xxxxxbytes loaded status message indicates the file was downloaded successfully. An Incompatible Hardware Type Error message indicates the configuration was not applied due to a hardware compatibility issue between the importing and exporting devices.

5 Click *Apply* to save the filename and Server IP information. The Apply button does not execute the import or export operation, only saves the settings entered.

6 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on Config Import/Export screen to the last saved configuration.

7 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Updating Device Firmware

Extreme Networks periodically releases updated versions of the access point device firmware to the Extreme Networks Web site. If the access point firmware version displayed on the *System Settings* page (see "Configuring System Settings" on page 78) is older than the version on the Web site, Extreme Networks recommends updating the access point to the latest firmware version for full feature functionality.

The Access Point's automatic update feature updates the Access Point's firmware and configuration file automatically when the Access Point is reset or when the Access Point initiates a DHCP request.

The firmware is automatically updated each time firmware versions are found to be different between what is running on the Access Point and the firmware file located on the server. The configuration file is automatically updated when the configuration file name on the server is different than the name of the file previously loaded on the Access Point or when the file version (on the server) is different than the version currently in use on the Access Point.

Additionally, the configuration version can be manually changed in the text file to cause the configuration to be applied when required. The parameter name within the configuration file is "cfg-version-1.1-01." The Access Point only checks the two characters after the third hyphen (01) when making a comparison. Change the last two characters to update the Access Point's configuration. The two characters can be alpha-numeric.

When downloading to a previous firmware version, all configuration settings are lost and the Access Point returns to factory default settings of the lower version.

CAUTION

If downgrading firmware from to a lower version, the Access Point automatically reverts to default settings of the lower version, regardless of whether you are downloading the firmware manually or using the automatic download feature. The automatic feature allows the user to download the configuration file at the same time, but since the firmware reverts to the default settings of the lower version, the configuration file is ignored.

For detailed update scenarios involving both a Windows DHCP and a Linux BootP server configuration, see "Configuring Automatic Updates using a DHCP or Linux BootP Server" on page 631.

CAUTION

Loaded and signed CA certificates will be lost when changing the Access Point's firmware version using either the GUI or CLI. After a certificate has been successfully loaded, export it to a secure location to ensure its availability after a firmware update.

If restoring the Access Point's factory default firmware, you must export the certificate file BEFORE restoring the Access Point's factory default configuration. Import the file back after the updated firmware is installed.

If a firmware update is required, use the *Firmware Update* screen to specify a filename and define a file location for updating the firmware.

NOTE

The firmware file must be available from a SFTP, FTP or TFTP site to perform the update.

CAUTION

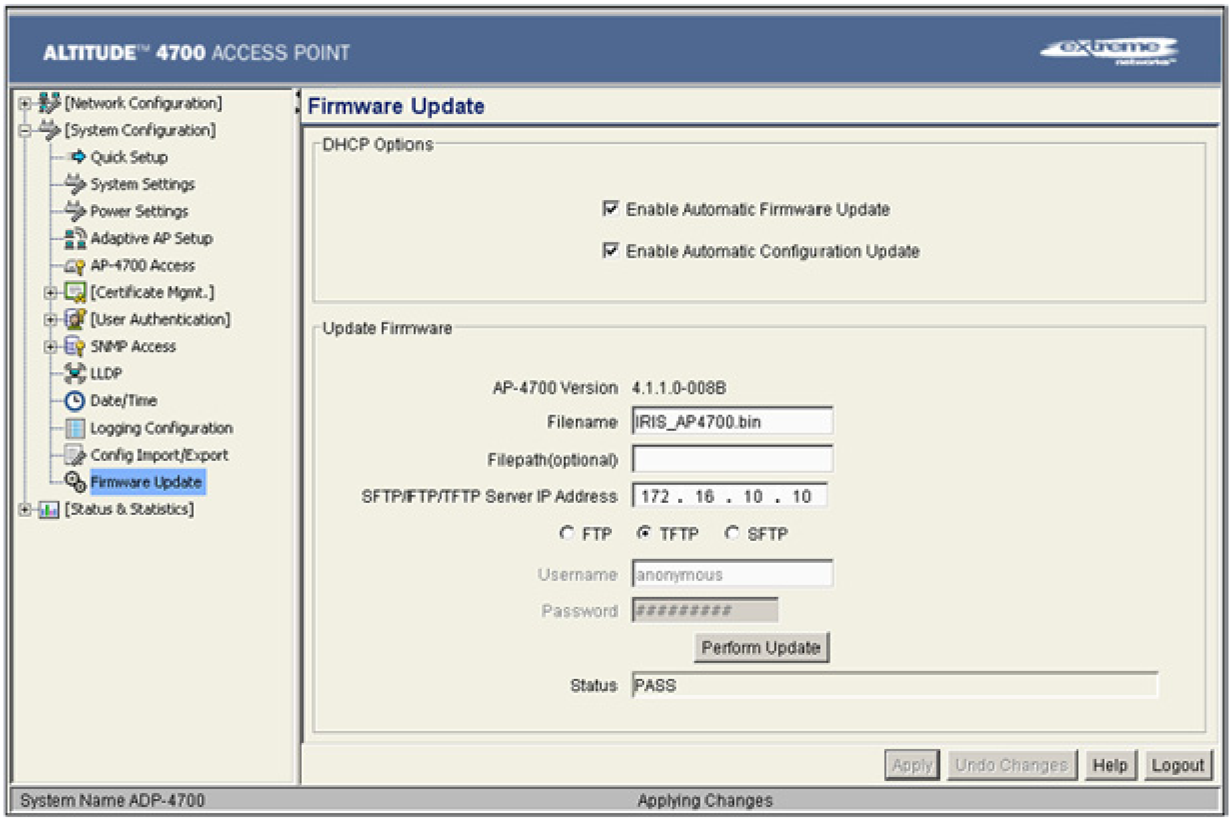
Make sure a copy of the access point's configuration is exported before updating the firmware.

To conduct a firmware update on the access point:

1 Export the access point current configuration settings before updating the firmware to have the most recent settings available after the firmware is updated.

Refer to "Importing/Exporting Configurations" on page 114 for instructions on exporting the access point's current configuration to have it available after the firmware is updated.

2 Select *System Configuration* > *Firmware Update* from the access point menu tree.



Firmware Update

DHCP Options

☑ Enable Automatic Firmware Update

☑ Enable Automatic Configuration Update

Update Firmware

AP-4700 Version 4.1.1.0-008B

Filename IRIS_AP4700.bin

Filepath(optional)

SFTP/FTP/TFTP Server IP Address 172 . 16 . 10 . 10

○ FTP ● TFTP ○ SFTP

Username anonymous

Password ##########

Status PASS

System Name ADP-4700

Applying Changes

3 Configure the *DHCP Options* checkboxes to enable/disable automatic firmware and/or configuration file updates.

DHCP options are used for out-of-the-box rapid deployment for Extreme Networks wireless products. The following are the two options available on the Access Point:

- Enable Automatic Firmware Update
- Enable Automatic Configuration Update

Both DHCP options are enabled by default.

These options can be used to update newer firmware and configuration files on the Access Point. For more information on how to configure a DHCP or BootP Server for the automatic upgrade process, see "Usage Scenarios" on page 631.

The update is conducted over the LAN or WAN port depending on which server responds first to the Access Point's request for an automatic update.

Enable Automatic Firmware Update — Enable this checkbox to allow an automatic firmware update when firmware versions are found to be different between what is running on the Access Point and the firmware that resides on the server. A firmware update will only occur if the Access Point is reset or when the Access Point does a DHCP request.

This feature is used in conjunction with DHCP/BootP options configured on a DHCP or BootP server.

If this checkbox is not enabled, the firmware update is required to be conducted manually.

Enable Automatic Configuration Update — Select this checkbox to allow an automatic configuration update when the configuration filenames are found to be different between the filename loaded on the Access Point and the configuration filename that resides on the server or when the configuration file versions are found to be different between the configuration file version loaded on the Access Point and the configuration file that resides on server. A configuration update will only occur if the Access Point is reset or when the Access Point does a DHCP request.

This feature is used in conjunction with DHCP/BootP options configured on a DHCP or BootP server.

If this checkbox is not enabled, the configuration update is required to be done manually.

CAUTION

If using a Linux server configured to support the BootP "bf" option, an automatic firmware update is not be triggered unless both the Enable Automatic Firmware Update and Enable Automatic Configuration Update options are selected. If the Configuration Update option is disabled, the Access Point will not download the configuration file. Without the configuration file, the Access Point cannot parse for the firmware file name required to trigger the firmware update.

If updating the Access Point manually, configure the *Update Firmware* fields as required to set a filename and target firmware file upload location for firmware updates.

4. Specify the name of the target firmware file within the *Filename* field.
5. If the target firmware file resides within a directory, specify a complete path for the file within the *Filepath(optional)* field.
6. Enter an IP address for the SFTP, FTP or TFTP server used for the update. Only numerical IP address names are supported, no DNS can be used.
7. Select *FTP*, *TFTP* or *SFTP* to define whether the firmware file resides on a FTP, TFTP or SFTP server.

8 Set the following parameters:

- *Username*—Specify a username for the FTP or SFTP server login.
- *Password*—Specify a password for FTP or SFTP server login. Default is admin123. A blank password is not supported.

NOTE

Click Apply to save the settings before performing the firmware update. The user is not able to navigate the access point user interface while the firmware update is in process.

9 Click the *Perform Update* button to initiate the update. Upon confirming the firmware update, the AP reboots and completes the update.

NOTE

The Access Point must complete the reboot process to successfully update the device firmware, regardless of whether the reboot is conducted using the GUI or CLI interfaces.

10 After the AP reboots, return to the Firmware Update screen. Check the *Status* field to verify whether the firmware update was successful. If an error occurs, one of the following error messages will display:

```
FAIL: auto fw update check
FAIL: network activity time out
FAIL: firmware check
FAIL: exceed memory limit
FAIL: authentication
FAIL: connection time out
FAIL: control channel error
FAIL: data channel error
FAIL: channel closed unexpected
FAIL: establish data channel
FAIL: accept data channel
FAIL: user interrupted
FAIL: no valid interface found
FAIL: conflict ip address
FAIL: command exchange time out
FAIL: invalid subnet number
```

11 Confirm the access point configuration is the same as it was before the firmware update. If they are not, restore the settings. Refer to "Importing/Exporting Configurations" on page 114 for instructions on exporting the configuration back to the access point.

12 Click *Apply* to save the filename and filepath information entered into the Firmware Update screen. The Apply button does not execute the firmware, only saves the update settings entered.

13 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on Firmware Update screen to the last saved configuration.

14 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

5 CHAPTER Network Management

Refer to the following for network management configuration activities supported by the Access Point user interface:

- Configuring the LAN Interface on page 123
- Configuring WAN Settings on page 135
- Enabling Wireless LANs (WLANs) on page 146
- Configuring Router Settings on page 186
- Configuring IP Filtering on page 188

Configuring the LAN Interface

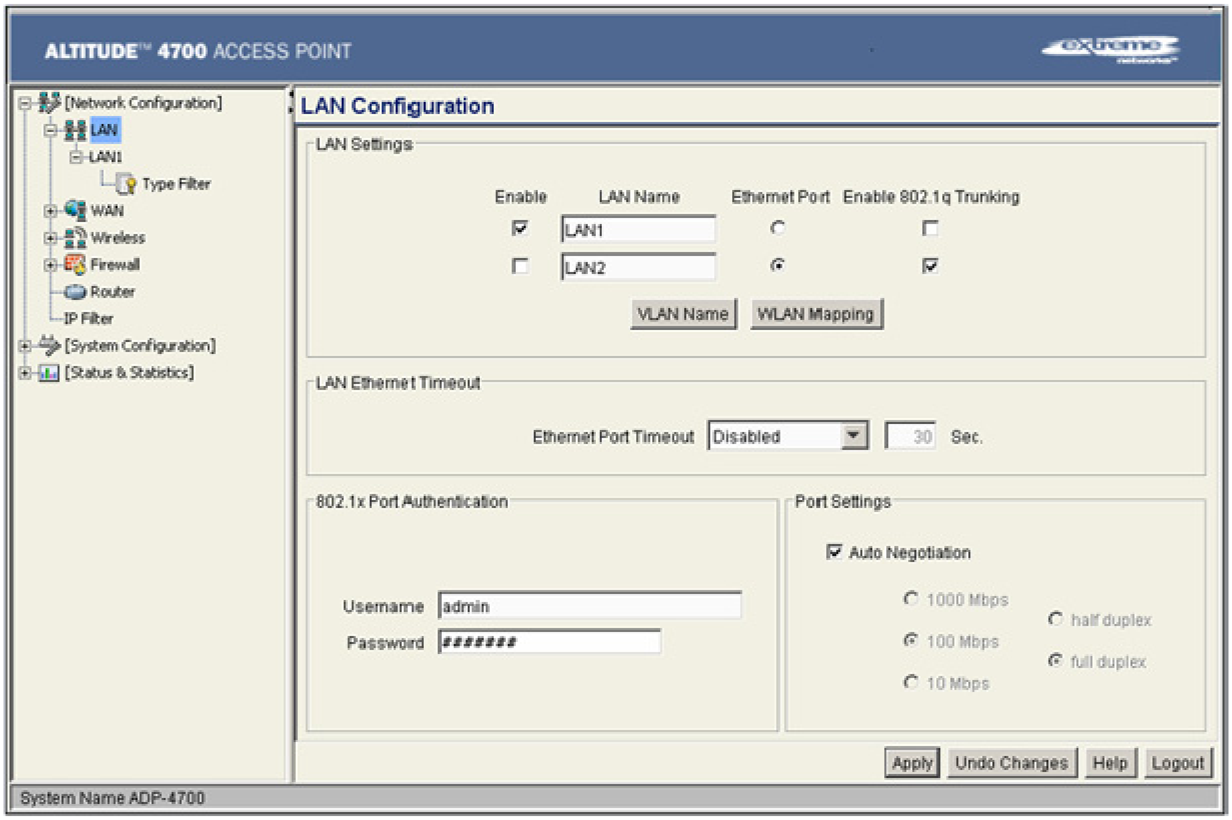
The access point has one physical LAN port supporting two unique LAN interfaces. The access point LAN port has its own MAC address. The LAN port MAC address is always the value of the access point WAN port MAC address plus 1. The LAN and WAN port MAC addresses can be located within the LAN and WAN Stats screens.

For information on locating the Access Point's MAC addresses, see "Viewing WAN Statistics" on page 263 and "Viewing LAN Statistics" on page 266.

Use the *LAN Configuration* screen to enable one (or both) of the Access Point's LAN interfaces, assign them names, define which LAN is currently active on the Access Point Ethernet port and assign a timeout value to disable the LAN connection if no data traffic is detected within a defined interval.

To configure the access point LAN interface:

1 Select *Network Configuration* > *LAN* from the access point menu tree.



LAN Configuration

LAN Settings

Enable	LAN Name	Ethernet Port	Enable 802.1q Trunking
☑	LAN1	○	□
□	LAN2	●	☑

LAN Ethernet Timeout

Ethernet Port Timeout: Disabled 30 Sec.

802.1x Port Authentication

Username: admin

Password: #######

Port Settings

☑ Auto Negotiation

○ 1000 Mbps
● 100 Mbps
○ 10 Mbps

○ half duplex
● full duplex

2 Configure the *LAN Settings* field to enable the access point LAN1 and/or LAN2 interface, assign a timeout value, enable 802.1q trunking, configure WLAN mapping and enable 802.1x port authentication.

Enable

Select the LAN1 and/or LAN2 checkbox to allow the forwarding of data traffic over the specified LAN connection. The LAN1 connection is enabled by default, but both LAN interfaces can be enabled simultaneously. The LAN2 setting is disabled by default.

LAN Name

Use the *LAN Name* field to modify the existing LAN name. LAN1 and LAN2 are the default names assigned to the LANs until modified by the user.

Ethernet Port

The *Ethernet Port* radio buttons allow you to select one of the two available LANs as the LAN actively transmitting over the Access Point's LAN port. Both LANs can be active at any given time, but only one can transmit over the Access Point's physical LAN connection, thus the selected LAN has priority.

Enable 802.1q Trunking

Select the *Enable 802.1q Trunking* checkbox to enable the LAN to conduct VLAN tagging. If selected, click the *WLAN Mapping* button to configure mappings between individual WLANs and LANs. If enabled, the Access Point is required to be connected to a trunked port.

VLAN Name

Click the *VLAN Name* button to launch the *VLAN Name* screen to create VLANs and assign them VLAN IDs.

WLAN Mapping

Click the *WLAN Mapping* button to launch the *VLAN Configuration* screen to map existing WLANs to one of the two LANs and define the WLAN's VLAN membership (up to 16 mappings are possible per Access Point).

3 Refer to the *LAN Ethernet Timeout* field to define how LAN Ethernet inactivity is processed by the Access Point.

Use the *Ethernet Port Timeout* drop-down menu to define how the Access Point interprets inactivity for the LAN assigned to the Ethernet port. When *Enabled* is selected, the Access Point uses the value defined in the *Sec.* box (default is 30 seconds). Selecting *Disabled* allows the LAN to use the Ethernet port for an indefinite timeout period. Select the *Hardware Detect* option to use the physical LAN port to detect activity. If the LAN port does not detect a physical connection, the radio is unavailable to the Access Point.

4 Refer to the *802.1x Port Authentication* field if using port authentication over the Access Point's LAN port.

The Access Point only supports 802.1x authentication over its LAN port. The Access Point behaves as an 802.1x supplicant to authenticate to a server on the network. If using 802.1x authentication, enter the authentication server user name and password. The default password is "admin123." For information on enabling and configuring authentication schemes on the Access Point, see "Enabling Authentication and Encryption Schemes" on page 200.

5 Use the *Port Settings* field to define how the Access Point manages throughput over the LAN port.

Auto Negotiation

Select the *Auto Negotiation* checkbox to enable the Access Point to automatically exchange information (over its LAN port) about data transmission speed and duplex capabilities.

Auto negotiation is helpful when using the Access Point in an environment where different devices are connected and disconnected on a regular basis.

Selecting Auto Negotiate disables the Mbps and duplex checkbox options.

1000 Mbps

Select this option to establish a 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the Access Point's LAN port. This option is not available if Auto Negotiation is selected.

100 Mbps

Select this option to establish a 100 Mbps data transfer rate for the selected half duplex or full duplex transmission over the Access Point's LAN port. This option is not available if Auto Negotiation is selected.

10 Mbps

Select this option to establish a 10 Mbps data transfer rate for the selected half duplex or full duplex transmission over the Access Point's LAN port. This option is not available if Auto Negotiation is selected.

half duplex

Select this option to transmit data to and from the Access Point, but not at the same time. Using a half duplex transmission, the Access Point can send data over its LAN port then immediately receive data from the same direction in which the data was transmitted. Like a full-duplex transmission, a half-duplex transmission can carry data in both directions, just not at the same time.

full duplex

Select this option to transmit data to and from the Access Point at the same time. Using full duplex, the Access Point can send data over its LAN port while receiving data as well.

6 Click *Apply* to save any changes to the LAN Configuration screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost if the prompts are ignored.

7 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the LAN configuration screen to the last saved configuration.

8 Click *Logout* to securely exit the access point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring VLAN Support

A *Virtual Local Area Network (VLAN)* is a means to electronically separate data on the same access point from a single broadcast domain into separate broadcast domains. The access point can group devices on one or more WLANs so that they can communicate as if they were attached to the same wire, when in fact they are located on a different LAN segment. Because VLANs are based on logical instead of physical connections, they are extremely flexible. By using a VLAN, you can group by logical function instead of physical location. A maximum of 16 VLANs can be supported on the Access Point. An administrator can map 16 WLANs to 16 VLANs and enable or disable dynamic VLAN assignment.

VLANs enable organizations to share network resources in various network segments within large areas (airports, shopping malls, etc.). A VLAN is a group of clients with a common set of requirements independent of their physical location. VLANs have the same attributes as physical LANs, but they enable system administrators to group MUs even when they are not members of the same network segment.

NOTE

A WLAN supporting a mesh network does not need to be assigned to a particular VLAN, as all the traffic proliferating the mesh network is already trunked. However, if MUs are to be connected to the Mesh WLAN, the WLAN will need to be tied to a VLAN.

The access point assignment of VLANs can be implemented using Static or Dynamic assignments (often referred to as memberships) for individual WLANs. Both methods have their advantages and disadvantages. Static VLAN membership is perhaps the most widely used method because of the relatively small administration overhead and security it provides. With Static VLANs, you manually assign individual WLANs to individual VLANs.

Although static VLANs are the most common form of VLAN assignments, dynamic VLAN assignment is possible per WLAN. Configuring dynamic VLANs entail the access point sending a DHCP request for device information (such as an IP address). Additional information (such as device MAC address information) is sent to the access point. The access point sends this MAC address to a host housing a copy of the Dynamic VLAN database. This database houses the records of MAC addresses and VLAN assignments. The VLAN database looks up the MAC to determine what VLAN is assigned to it. If it is not in the database, it simply uses a default VLAN assignment. The VLAN assignment is sent to the access point. The access point then maps the target WLAN for the assigned VLAN and traffic passes normally, allowing for the completion of the DHCP request and further traffic.

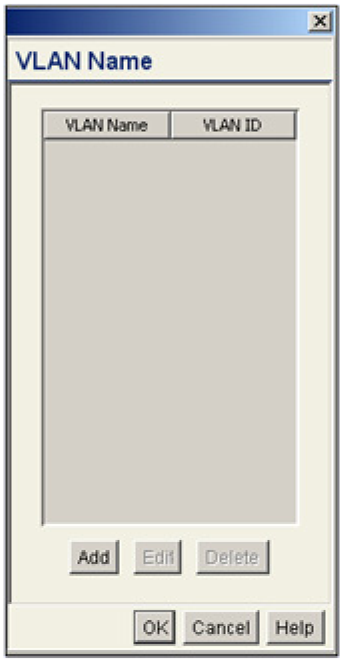
To create new VLANs or edit the properties of an existing VLAN:

1 Select *Network Configuration > LAN* from the access point menu tree.

2 Ensure the *Enable 802.1q Trunking* button is selected from within the LAN Setting field.

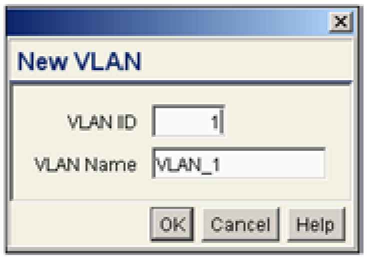
Trunk links are required to pass VLAN information between destinations. A trunk port is by default a member of all the VLANs existing on the access point and carry traffic for all those VLANs. Trunking is a function that must be enabled on both sides of a link.

3 Select the *VLAN Name* button.



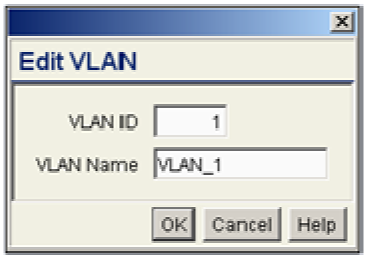
The VLAN name screen displays. The first time the screen is launched a default VLAN name of 1 and a default VLAN ID of 1 display. The VLAN name is auto-generated once the user assigns a VLAN ID. However, the user has the option of re-assigning a name to the VLAN using *New VLAN* and *Edit VLAN* screens.

To create a new VLAN, click the *Add* button. To edit the properties of an existing VLAN, click the *Edit* button.



VLAN ID 1

VLAN Name VLAN_1



VLAN ID 1

VLAN Name VLAN_1

4 Assign a unique *VLAN ID* (from 1 to 4095) to each VLAN added or modified.

The VLAN ID associates a frame with a specific VLAN and provides the information the access point needs to process the frame across the network. Therefore, it may be practical to assign a name to a VLAN representative or the area or type of network traffic it represents.

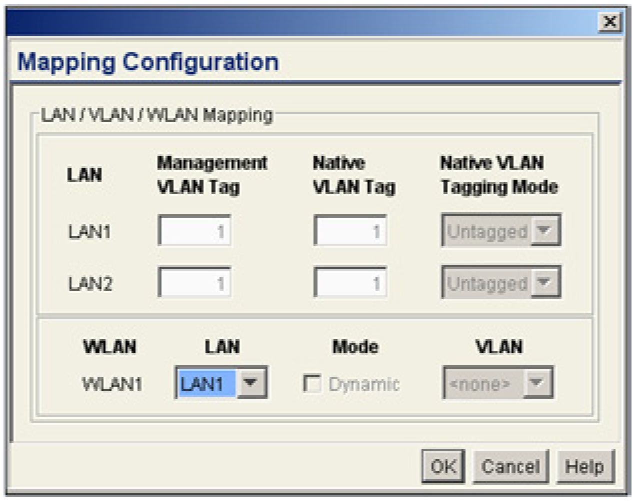
A business may have offices in different locations and want to extend an internal LAN between the locations. An access point managed infrastructure could provide this connectivity, but it requires VLAN numbering be managed carefully to avoid conflicts between two VLANs with the same ID.

5 Define a 32 character maximum *VLAN Name*.

Enter a unique name that identifies members of the VLAN. Extreme Networks recommends selecting the name carefully, as the VLAN name should signify a group of clients with a common set of requirements independent of their physical location.

6 Click *Apply* to save the changes to the new or modified VLAN.

7 From the LAN Configuration screen, click the *WLAN Mapping* button. The *Mapping Configuration* screen displays.



Mapping Configuration

LAN / VLAN / WLAN Mapping

LAN	Management VLAN Tag	Native VLAN Tag	Native VLAN Tagging Mode
LAN1	1	1	Untagged
LAN2	1	1	Untagged

WLAN	LAN	Mode	VLAN
WLAN1	LAN1	□ Dynamic	<none>

8 Enter a *Management VLAN Tag* for LAN1 and LAN2.

The Management VLAN uses a default tag value of 1. The Management VLAN is used to distinguish VLAN traffic flows for the LAN. The trunk port marks the frames with special tags as they pass between the access point and its destination, these tags help distinguish data traffic.

Authentication servers (such as RADIUS and Kerberos) must be on the same Management VLAN. Additionally, DHCP and BOOTP servers must be on the same Management VLAN as well.

9 Define a *Native VLAN Tag* for LAN1 and LAN2.

A trunk port configured with 802.1Q tagging can receive both tagged and untagged traffic. By default, the Access Point forwards untagged traffic with the native VLAN configured for the port. The Native VLAN is VLAN 1 by default. Extreme Networks suggests leaving the Native VLAN set to 1 as other layer 2 devices also have their Native VLAN set to 1.

10 Use the *Native VLAN Tagging Mode* drop-down menu to define whether the native VLAN applies a tag to traffic.

A tagged VLAN uses an extra tag in the MAC header to identify a frame's VLAN membership. This tag helps define the VLAN and QoS priority. A tagged frame is four bytes longer than an untagged frame and contains two bytes of *Tag Protocol Identifier* (TPID) information within the type and length field of an Ethernet frame and two bytes of *Tag Control Information* (TCI) after the Ethernet frame's source address field.

When *Tagged* is selected from the drop-down menu, the Access Point forwards all tagged frames in the native VLAN and admits only tagged frames on trunks. When Tagged is selected the Access Point drops any untagged traffic, including untagged traffic in the native VLAN. *Untagged* is selected by default.

11 Use the *LAN* drop-down menu to map one of the two LANs to the WLAN listed to the left. With this assignment, the WLAN uses this assigned LAN interface.

12 Select the *Dynamic* checkboxes (under the *Mode* column) to configure the VLAN mapping as a dynamic VLAN.

Using Dynamic VLAN assignments, a *VMPS (VLAN Management Policy Server)* dynamically assigns VLAN ports. The access point uses a separate server as a VMPS server. When a frame arrives on the access point, it queries the VMPS for the VLAN assignment based on the source MAC address of the arriving frame.

If statically mapping VLANs, leave the *Dynamic* checkbox specific to the target WLAN and its intended VLAN unselected. The administrator is then required to configure VLAN memberships manually.

The Dynamic checkbox is enabled only when a WLAN is having EAP configured. Otherwise, the checkbox is disabled.

13 Use the *VLAN* drop-down menu to select the name of the target VLAN to map to the WLAN listed on the left-hand side of the screen.

Extreme Networks recommends mapping VLANs strategically in order to keep VLANs tied to the discipline they most closely match. For example, If WLAN1 is comprised of MUs supporting the sales area, then WLAN1 should be mapped to sales if a sales VLAN has been already been created.

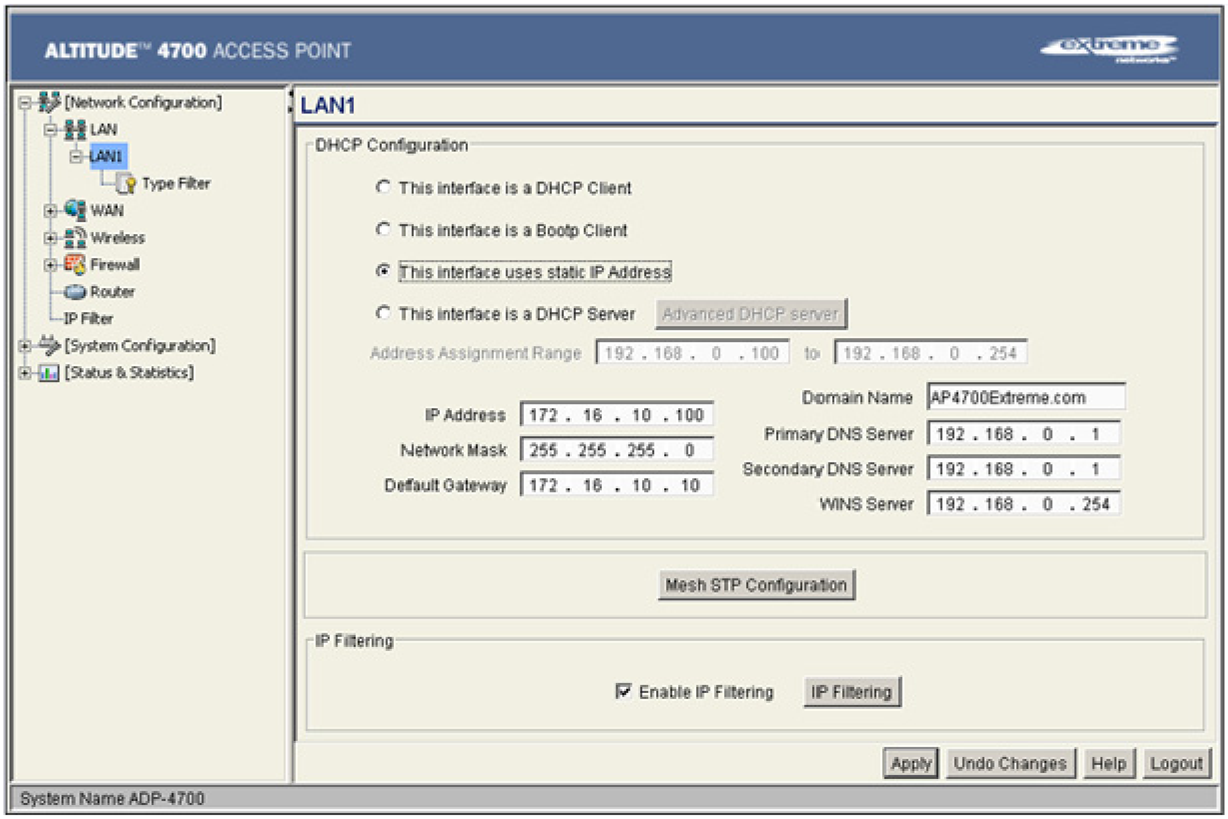
14 Click *Apply* to return to the *VLAN Name* screen. Click *OK* to return to the LAN screen. Once at the LAN screen, click *Apply* to re-apply your changes.

Configuring LAN1 and LAN2 Settings

Both LAN1 and LAN2 have separate sub-screens to configure the DHCP settings used by the LAN1 and LAN2 interfaces. Within each LAN screen is a button to access a sub-screen to configure advanced DHCP settings for that LAN. For more information, see "Configuring Advanced DHCP Server Settings" on page 132. Additionally, LAN1 and LAN2 each have separate *Type Filter* submenu items used to prevent specific (an potentially unnecessary) frames from being processed, for more information, see "Setting the Type Filter Configuration" on page 133.

To configure unique settings for either LAN1 or LAN2:

1 Select *Network Configuration > LAN > LAN1 (or LAN2)* from the access point menu tree.



LAN1

DHCP Configuration

○ This interface is a DHCP Client

○ This interface is a Bootp Client

● This interface uses static IP Address

○ This interface is a DHCP Server

Address Assignment Range 192 . 168 . 0 . 100 to 192 . 168 . 0 . 254

IP Address	172 . 16 . 10 . 100	Domain Name	AP4700Extreme.com
Network Mask	255 . 255 . 255 . 0	Primary DNS Server	192 . 168 . 0 . 1
Default Gateway	172 . 16 . 10 . 10	Secondary DNS Server	192 . 168 . 0 . 1
		WINS Server	192 . 168 . 0 . 254

IP Filtering

☑ Enable IP Filtering

System Name ADP-4700

2 Configure the *DHCP Configuration* field to define the DHCP settings used for the LAN.

NOTE

When setting the LAN interface to be a DHCP Server and adding an IP address, the primary DNS IP address might not be updated, with only the secondary address getting updated. Ensure the primary address is the same as the IP address of the LAN.

NOTE

Extreme Networks recommends the WAN and LAN ports should not both be configured as DHCP clients.

This interface is a DHCP Client

Select this button to enable DHCP to set network address information via this LAN1 or LAN2 connection. This is recommended if the access point resides within a large corporate network or the *Internet Service Provider (ISP)* uses DHCP. This setting is enabled for LAN1 by default.

DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. If DHCP Client is selected, the first DHCP or BOOTP server to respond sets the IP address and network address values since DHCP and BOOTP are interoperable.

This interface is a BOOTP Client

Select this button to enable BOOTP to set access point network address information via this LAN1 or LAN2 connection.

When selected, only BOOTP responses are accepted by the access point. If both DHCP and BOOTP services are required, do not select BOOTP Client.

This interface uses static IP Address

Select the *This interface uses static IP Address* button, and manually enter static network address information in the areas provided.

This interface is a DHCP Server

The access point can be configured to function as a DHCP server over the LAN1 or LAN2 connection. Select the *This interface is a DHCP Server* button and manually enter static network address information in the areas provided.

Address Assignment Range

Use the address assignment parameter to specify a range of numerical (non DNS name) IP addresses reserved for mapping client MAC addresses to IP addresses. If a manually (static) mapped IP address is within the IP address range specified, that IP address could still be assigned to another client. To avoid this, ensure all statically mapped IP addresses are outside of the IP address range assigned to the DHCP server.

Advanced DHCP Server

Click the *Advanced DHCP Server* button to display a screen used for generating a list of static MAC to IP address mappings for reserved clients. A separate screen exists for each of the LANs. For more information, see “Configuring Advanced DHCP Server Settings” on page 132.

IP Address

The network-assigned numerical (non DNS name) IP address of the access point.

Network Mask

The first two sets of numbers specify the network domain, the next set specifies the subset of hosts within a larger network. These values help divide a network into subnetworks and simplify routing and data transmission. The subnet mask defines the size of the subnet.

Default Gateway

The *Default Gateway* parameter defines the numerical (non DNS name) IP address of a router the access point uses on the Ethernet as its default gateway.

Domain Name

Enter the name assigned to the primary DNS server.

Primary DNS Server

Enter the Primary DNS numerical (non DNS name) IP address.

Secondary DNS Server

Extreme Networks recommends entering the numerical IP address of an additional DNS server (if available), used if the primary DNS server goes down. A maximum of two DNS servers can be used.

WINS Server
Enter the numerical (non DNS name) IP address of the WINS server. WINS is a Microsoft NetBIOS name server. Using a WINS server eliminates the broadcasts needed to resolve computer names to IP addresses by providing a cache or database of translations.

Mesh STP Configuration
Click the *Mesh STP Configuration* button to define bridge settings for this specific LAN. Each of the Access Point's two LANs can have a separate mesh configuration. As the *Spanning Tree Protocol* (STP) mentions, each mesh network maintains hello, forward delay and max age timers. These settings can be used as is using the current default settings, or be modified. However, if these settings are modified, they need to be configured for the LAN connecting to the mesh network WLAN.

3 Refer to the *IP Filtering* field to optionally enable the IP filtering feature, and (if enabled) apply existing IP filters (and their rules and permissions) to LAN1 or LAN2.

Enable IP Filtering
Selecting this checkbox allows the LAN to employ filter policies and rules to determine which IP packets are processed normally over the LAN and which are discarded. If discarded, a packet is deleted and ignored (as if never received).

IP Filtering
Select the IP Filtering button to display a screen where existing IP filter policies can be applied to the LAN to allow or deny IP packets in either an incoming or outgoing direction based on the rules defined for the policy.

NOTE

For an overview of IP Filtering and how to create a filter, see "Configuring IP Filtering" on page 188. For information on applying an existing filter to the IP packet flow of a WLAN, see "Applying a Filter to LAN1, LAN2 or a WLAN (1-16)" on page 191.

4 Click *Apply* to save any changes to the LAN1 or LAN2 screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost if the prompts are ignored.

5 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the LAN1 or LAN2 screen to the last saved configuration.

6 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring Advanced DHCP Server Settings

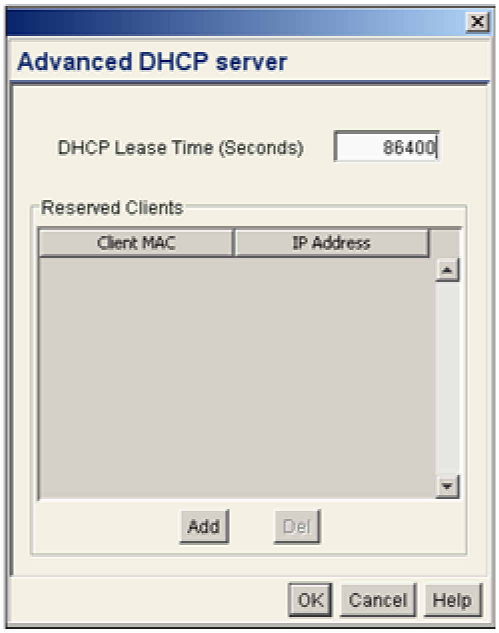
Use the *Advanced DHCP Server* screen to specify (reserve) static (or fixed) IP addresses for specific devices. Every wireless, 802.11x-standard device has a unique *Media Access Control (MAC)* address. This address is the device's hard-coded hardware number (shown on the bottom or back). An example of a MAC address is 00:A0:F8:45:9B:07.

The DHCP server can grant an IP address for as long as it remains in active use. The lease time is the number of seconds an IP address is reserved for re-connection after its last use. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than available IP addresses. This is useful, for example, in education and customer environments where MU users change frequently. Use longer leases if there are fewer users.

To generate a list of client MAC address to IP address mappings for the access point:

1 Select *Network Configuration > LAN > LAN1 (or LAN2)* from the access point menu tree.

2 Click the *Advanced DHCP Server* button from within the *LAN1* or *LAN2* screen.



Advanced DHCP server

DHCP Lease Time (Seconds) 86400

Reserved Clients

Client MAC	IP Address

3 Specify a lease period in seconds for available IP addresses using the *DHCP Lease Time (Seconds)* parameter. An IP address is reserved for re-connection for the length of time you specify. The default interval is 86400 seconds.

4 Click the *Add* button to create a new table entry within the *Reserved Clients* field.

If a statically mapped IP address is within the IP address range in use by the DHCP server, that IP address may still be assigned to another client. To avoid this, ensure all statically mapped IP addresses are outside of the IP address range assigned to the DHCP server.

If multiple entries exist within the Reserved Clients field, use the scroll bar to the right of the window to navigate.

5 Click the *Del* (delete) button to remove a selected table entry.

6 Click *OK* to return to the LAN1 or LAN2 page, where the updated settings within the *Advanced DHCP Server* screen can be saved by clicking the *Apply* button.

7 Click *Cancel* to undo any changes made. Undo Changes reverts the settings displayed to the last saved configuration.

Setting the Type Filter Configuration

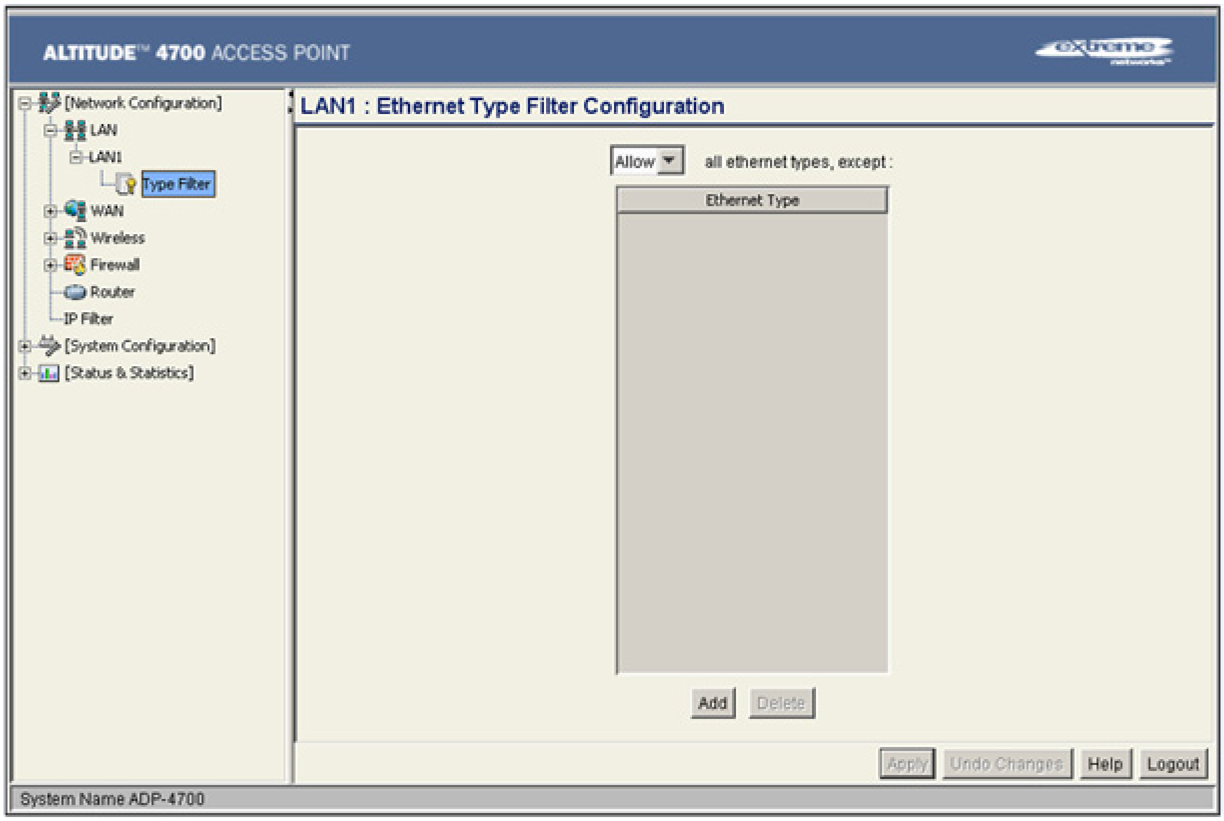
Each access point LAN (either LAN1 or LAN2) can keep a list of frame types that it forwards or discards. The Type Filtering feature prevents specific (and potentially unnecessary) frames from being processed by the access point in order to improve throughput. These include certain broadcast frames from devices that consume bandwidth, but are unnecessary to access point operations.

Use the *Ethernet Type Filter Configuration* screen to build a list of filter types and configure them as either allowed or denied for use with the this particular LAN.

To configure type filtering on the access point:

1 Select *Network Configuration* > *LAN* > *LAN1 (or LAN2)* > *Type Filter* from the access point menu tree.

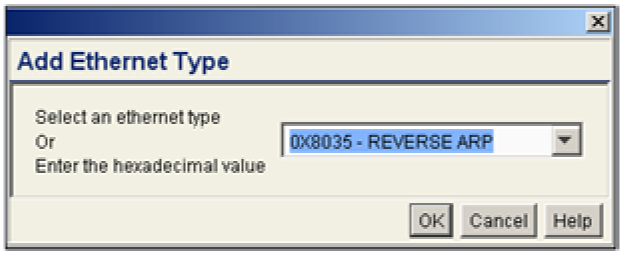
   The *Ethernet Type Filter Configuration* screen displays for the LAN. No Ethernet types are displayed (by default) when the screen is first launched.



2 Use the *all ethernet types, except* drop-down menu to designate whether the Ethernet Types defined for the LAN are allowed or denied for use by the access point.

3 To add an Ethernet type, click the *Add* button.

   The *Add Ethernet Type* screen displays. Use this screen to add one type filter option at a time, for a list of up to 16 entries.



   Packet types supported for the type filtering function include 16-bit DIX Ethernet types as well as Extreme Networks proprietary types. Select an Ethernet type from the drop down menu, or enter the Ethernet type's hexadecimal value. See your System Administrator if unsure of the implication of adding or omitting a type from the list for either LAN1 or LAN2.

4 To optionally delete a type filtering selection from the list, highlight the packet type and click the *Delete* button.

5 Click *Apply* to save any changes to the LAN1 or LAN2 Ethernet Type Filter Configuration screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

6 Click *Cancel* to securely exit the LAN1 or LAN2 Ethernet Type Filter Configuration screen without saving your changes.

7 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring WAN Settings

A *Wide Area Network (WAN)* is a widely dispersed telecommunications network. The access point includes one WAN port. The access point WAN port has its own MAC address. In a corporate environment, the WAN port might connect to a larger corporate network. For a small business, the WAN port might connect to a DSL or cable modem to access the Internet.

The Altitude 4710 Access Point supports an express card slot that can provide a secondary link in the event of a wired WAN failure. The Altitude 4710's wired WAN is the primary WAN link, as long as it's enabled and connected, and the WWAN interface functions as the secondary link.

For the WWAN to be a viable recovery solution, an Altitude 4710 must monitor the link status of the wired WAN and check the health of the connection. If the Altitude 4710 detects the loss of the wired WAN connection, it establishes the WWAN connection and updates the default gateway to the WWAN interface. Additionally, the NAT rule is changed dynamically from the wired WAN interface to the wireless WAN interface. All traffic that used go to the wired WAN is redirected to the WWAN. If the Altitude 4710 detects the wired WAN link is restored and up for at least 1 minute, the operation is reversed. The wired WAN becomes the default WAN link once again.

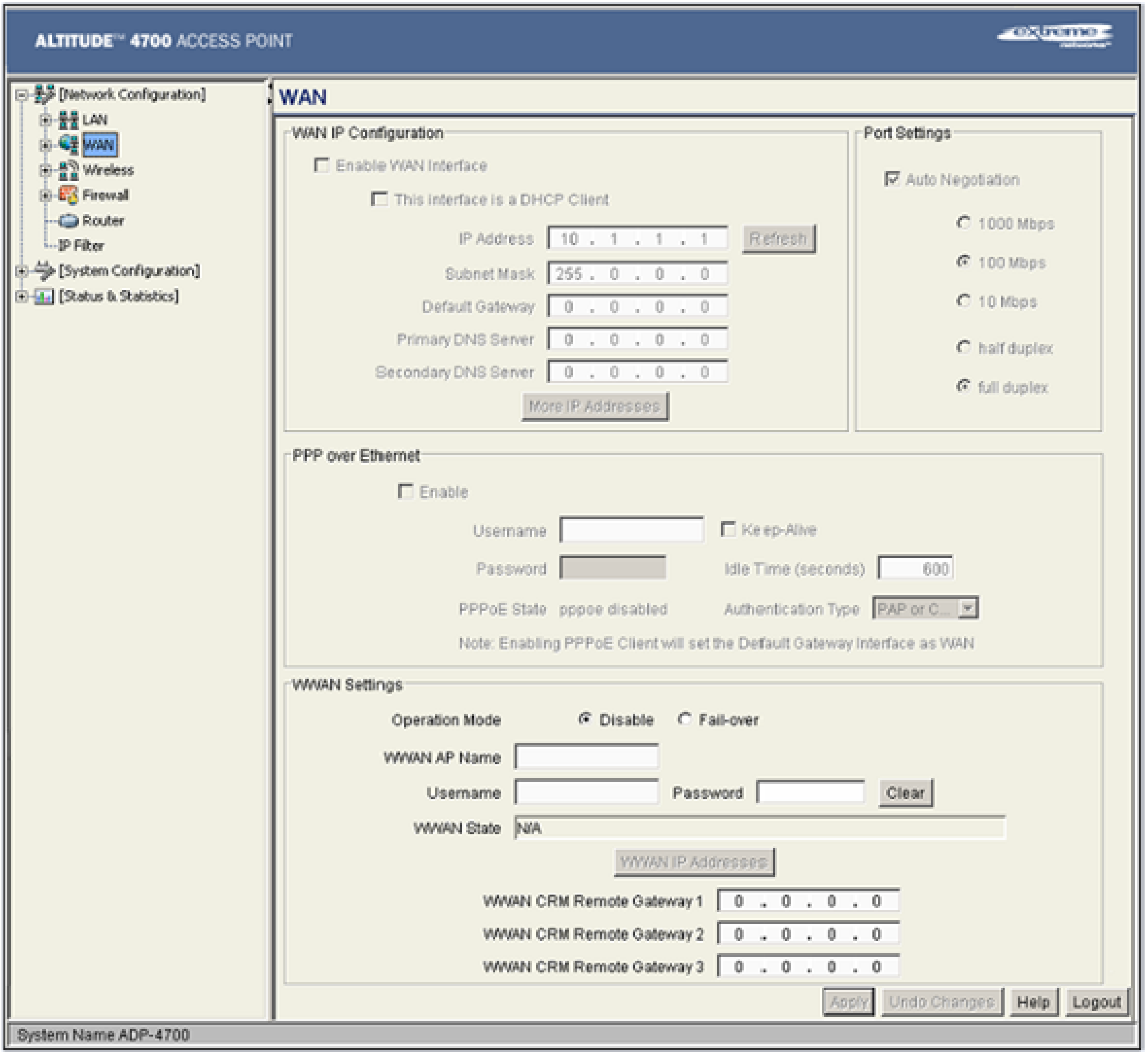
Use the *WAN* screen to set the WAN IP configuration, *Point-to-Point Protocol over Ethernet (PPPoE)* parameters and the Altitude 4710.

NOTE

The WAN port is not enabled until the AP4700 is powered by an 802.3at POE supply.

To configure WAN settings for the access point:

1 Select *Network Configuration* > *WAN* from the access point menu tree.



WAN IP Configuration

□ Enable WAN Interface

□ This interface is a DHCP Client

IP Address 10 . 1 . 1 . 1

Subnet Mask 255 . 0 . 0 . 0

Default Gateway 0 . 0 . 0 . 0

Primary DNS Server 0 . 0 . 0 . 0

Secondary DNS Server 0 . 0 . 0 . 0

Port Settings

☑ Auto Negotiation

○ 1000 Mbps

● 100 Mbps

○ 10 Mbps

○ half duplex

● full duplex

PPP over Ethernet

□ Enable

Username

□ Keep-Alive

Password

Idle Time (seconds) 600

PPPoE State pppoe disabled

Authentication Type PAP or C...

Note: Enabling PPPoE Client will set the Default Gateway Interface as WAN

WWAN Settings

Operation Mode ● Disable ○ Fail-over

WWAN AP Name

Username

Password

WWAN State N/A

WWAN CRM Remote Gateway 1 0 . 0 . 0 . 0

WWAN CRM Remote Gateway 2 0 . 0 . 0 . 0

WWAN CRM Remote Gateway 3 0 . 0 . 0 . 0

System Name ADP-4700

2 Refer to the *WAN IP Configuration* field to enable the WAN interface, and set network address information for the WAN connection.

NOTE

Extreme Networks recommends that the WAN and LAN ports should not both be configured as DHCP clients.

Enable WAN Interface	Select the *Enable WAN Interface* checkbox to enable a connection between the access point and a larger network or outside world through the WAN port. Disable this option to effectively isolate the access point's WAN. No connections to a larger network or the Internet are possible. MUs cannot communicate beyond the LAN. By default, the WAN port is static with an IP address of 10.1.1.1.
This interface is a DHCP Client	This checkbox enables DHCP for the access point WAN connection. This is useful, if the larger corporate network or *Internet Service Provider (ISP)* uses DHCP. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway. If DHCP client mode is enabled, the other WAN IP configuration parameters are grayed out.
IP Address	Specify a numerical (non DNS name) IP address for the access point's WAN connection. This address defines the AP's presence on a larger network or on the Internet. Obtain a static (dedicated) IP address from the ISP or network administrator. An IP address uses a series of four numbers expressed in dot notation, for example, 190.188.12.1.
Subnet Mask	Specify a subnet mask for the access point's WAN connection. This number is available from the ISP for a DSL or cable-modem connection, or from an administrator if the access point connects to a larger network. A subnet mask uses a series of four numbers expressed in dot notation (similar to an IP address). For example, 255.255.255.0 is a valid subnet mask.
Default Gateway	Specify the gateway address for the access point's WAN connection. The ISP or a network administrator provides this address.
Primary DNS Server	Specify the address of a primary *Domain Name System (DNS)* server. The ISP or a network administrator provides this address. A DNS server translates a domain name (for example, www.extremenetworks.com) into an IP address that networks can use.
Secondary DNS Server	Specify the address of a secondary DNS server if one is used. A secondary address is recommended if the primary DNS server goes down.

More IP Addresses

Click the *More IP Addresses* button to specify additional static IP addresses for the access point. Additional IP addresses are required when users within the WAN need dedicated IP addresses, or when servers need to be accessed (addressed) by the outside world. The More IP Addresses screen allows the administrator to enter up to seven additional WAN IP addresses for the access point WAN. Only numeric, non-DNS names can be used.

If PPP over Ethernet is enabled from within the WAN screen, the *VPN WAN IP Configuration* portion of the More IP Addresses screen is enabled. Enter the IP address and subnet mask used to provide the PPPoE connection over the Access Point's WAN port. Ensure the IP address is a numerical (non DNS) name.

Refresh

Click the *Refresh* button to update the network address information displayed within the WAN IP Configuration field.

3 Use the *Port Settings* field to define how the Access Point manages throughput over the WAN port.

Auto Negotiation

Select the *Auto Negotiation* checkbox to enable the Access Point to automatically exchange information (over its WAN port) about data transmission speed and duplex capabilities.

Auto negotiation is helpful when using the Access Point in an environment where different devices are connected and disconnected on a regular basis.

Selecting Auto Negotiate disables the Mbps and duplex checkbox options.

1000 Mbps

Select this option to establish a 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the Access Point's LAN port. This option is not available if Auto Negotiation is selected.

100 Mbps

Select this option to establish a 100 Mbps data transfer rate for the selected half duplex or full duplex transmission over the Access Point's WAN port. This option is not available if Auto Negotiation is selected.

10 Mbps

Select this option to establish a 10 Mbps data transfer rate for the selected half duplex or full duplex transmission over the Access Point's WAN port. This option is not available if Auto Negotiation is selected.

half duplex

Select this option to transmit data to and from the Access Point, but not at the same time. Using a half duplex transmission, the Access Point can send data over its WAN port then immediately receive data from the same direction in which the data was transmitted. Like a full-duplex transmission, a half-duplex transmission can carry data in both directions, just not at the same time.

full duplex

Select this option to transmit data to and from the Access Point at the same time. Using full duplex, the Access Point can send data over its WAN port while receiving data as well.

4 Configure the *PPP over Ethernet* field to enable high speed dial-up connections to the access point WAN port.

NOTE

Be aware that the Access Point can (incorrectly) carry over previously configured static IP information and maintain two connected routes once it gets an IP address from a PPPOE connection.

Enable	Use the checkbox to enable *Point-to-Point over Ethernet (PPPoE)* for a high-speed connection that supports this protocol. Most DSL providers are currently using or deploying this protocol. PPPoE is a data-link protocol for dialup connections. PPPoE allows a host PC to use a broadband modem (DSL) for access to high-speed data networks.
Username	Specify a username entered when connecting to the ISP. When the Internet session begins, the ISP authenticates the username.
Password	Specify a password entered when connecting to the ISP. When the Internet session starts, the ISP authenticates the password.
PPPoE State	Displays the current connection state of the PPPoE client. When a PPPoE connection is established, the status displays *Connected.* When no PPPoE connection is active, the status displays *Disconnected*.
Keep-Alive	Select the *Keep-Alive* checkbox to maintain the WAN connection indefinitely (no timeout interval). Some ISPs terminate inactive connections. Enabling Keep-Alive keeps the access point’s WAN connection active, even when there is no traffic. If the ISP drops the connection after an idle period, the access point automatically re-establishes the connection to the ISP. Enabling Keep-Alive mode disables (grays out) the *Idle Time* field.
Idle Time (seconds)	Specify an idle time in seconds to limit how long the access point’s WAN connection remains active after outbound and inbound traffic is not detected. The Idle Time field is grayed out if *Keep-Alive* is enabled.
Authentication Type	Use the *Authentication Type* menu to specify the authentication protocol(s) for the WAN connection. Choices include *None, PAP or CHAP, PAP,* or *CHAP.* *Password Authentication Protocol (PAP)* and *Challenge Handshake Authentication Protocol (CHAP)* are competing identify-verification methods. *PAP* sends a username and password over a network to a server that compares the username and password to a table of authorized users. If the username and password are matched in the table, server access is authorized. WatchGuard products do not support the PAP protocol because the username and password are sent as clear text that a hacker can read. *CHAP* uses secret information and mathematical algorithms to send a derived numeric value for login. The login server knows the secret information and performs the same mathematical operations to derive a numeric value. If the results match, server access is authorized. After login, one of the numbers in the mathematical operation is changed to secure the connection. This prevents any intruder from trying to copy a valid authentication session and replaying it later to log in.

5 Refer to the *WWAN Settings* field (located at the bottom of the WAN screen) to enable WWAN failover operation and define user names and passwords for WWAN card users.

The following express cards can be used with an Altitude 4710 to support the WAN failover feature:

NOTE

Failover from LAN to 3G is also supported.

- Verizon Wireless V740 ExpressCard
- GlobeTrotter Express HSUPA from Options
- Novatel Merlin 870
- Vodafone (Options) E3730 3G Broadband Express Card
- Telstra Turbo 7 Series Express Card (Aircard 880E)

NOTE

Extreme Networks recommends express cards be initially activated on a Windows machine using a SIM card subscribed to an appropriate service plan.

Operation Mode — Enable WWAN failover by selecting the *Fail-over* radio button. *Disable* is selected by default, meaning there's no WWAN card failover to the Altitude 4710's express card until Fail-over is selected and the Altitude 4710 can read the express card's modules during a boot up runtime operation.

Username — Specify a username entered when connecting to the ISP supporting the express card. When the Internet session begins, the ISP authenticates the username. The username cannot exceed 48 characters.

Password — Specify a password entered when connecting to the ISP supporting the express card. When the Internet session starts, the ISP authenticates the password. The password cannot exceed 40 characters.

WWAN State — Refer to the WWAN State field to discern whether the current Altitude 4710 power budget supports WWAN failover support.

WWAN IP Addresses — Click the *WWAN IP Addresses* button to specify additional static IP addresses for the WWAN. Additional IP addresses are required when users within the WWAN need dedicated IP addresses, or when servers need to be accessed (addressed) by the outside world. Only numeric, non-DNS names can be used.

WWAN CRM Remote Gateway 1 — Define a numerical IP address for this first WWAN remote gateway. If the Access Point detects the loss of the wired WAN connection, it establishes the WWAN connection and uses a remote gateway to route traffic. Traffic that used go to the wired WAN is redirected to the WWAN over this first choice remote gateway.

WWAN CRM Remote Gateway 2 — Optionally define a numerical IP address for a second WWAN remote gateway. If the Access Point detects the loss of the wired WAN connection, it establishes the WWAN connection and uses a remote gateway to route traffic. Traffic that used go to the wired WAN is redirected to the WWAN over this second choice remote gateway, if the first gateway is unavailable.

WWAN CRM Remote Gateway 3	Optionally define a numerical IP address for a third WWAN remote gateway. If the Access Point detects the loss of the wired WAN connection, it establishes the WWAN connection and uses a remote gateway to route traffic. Traffic that used go to the wired WAN is redirected to the WWAN over this third choice remote gateway, if the first two gateways addresses prove unavailable.
Tunnel Required	Select this option to use a remote tunnel with the Access Point's WWAN failover operations if the wired WAN connection is lost.
Tunnel Remote IP	If using a tunnel, provide a numerical IP address for the remote tunnel used by the Access Point's WWAN.
Tunnel Phrase	If using a tunnel, provide a passphrase used to secure the tunnel's connection to the Access Point's WWAN.

CAUTION

Both the Altitude 4710's WAN port and express card slot are disabled if the power mode is set to 3af, or if the Altitude 4710 defines its power budget as 3af. Refer to the Power Settings screen (go to "Configuring Power Settings" on page 81) or check the WWAN State (within the WAN screen) to determine whether the AP has sufficient power for the express card operation.

6 Click *Apply* to save any changes to the WAN screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

7 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the WAN screen to the last saved configuration.

8 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring Network Address Translation (NAT) Settings

Network Address Translation (NAT) converts an IP address in one network to a different IP address or set of IP addresses in another network. The access point router maps its local (inside) network addresses to WAN (outside) IP addresses, and translates the WAN IP addresses on incoming packets to local IP addresses. NAT is useful because it allows the authentication of incoming and outgoing requests, and minimizes the number of WAN IP addresses needed when a range of local IP addresses is mapped to each WAN IP address. NAT can be applied in one of two ways:

- One-to-one mapping with a private side IP address

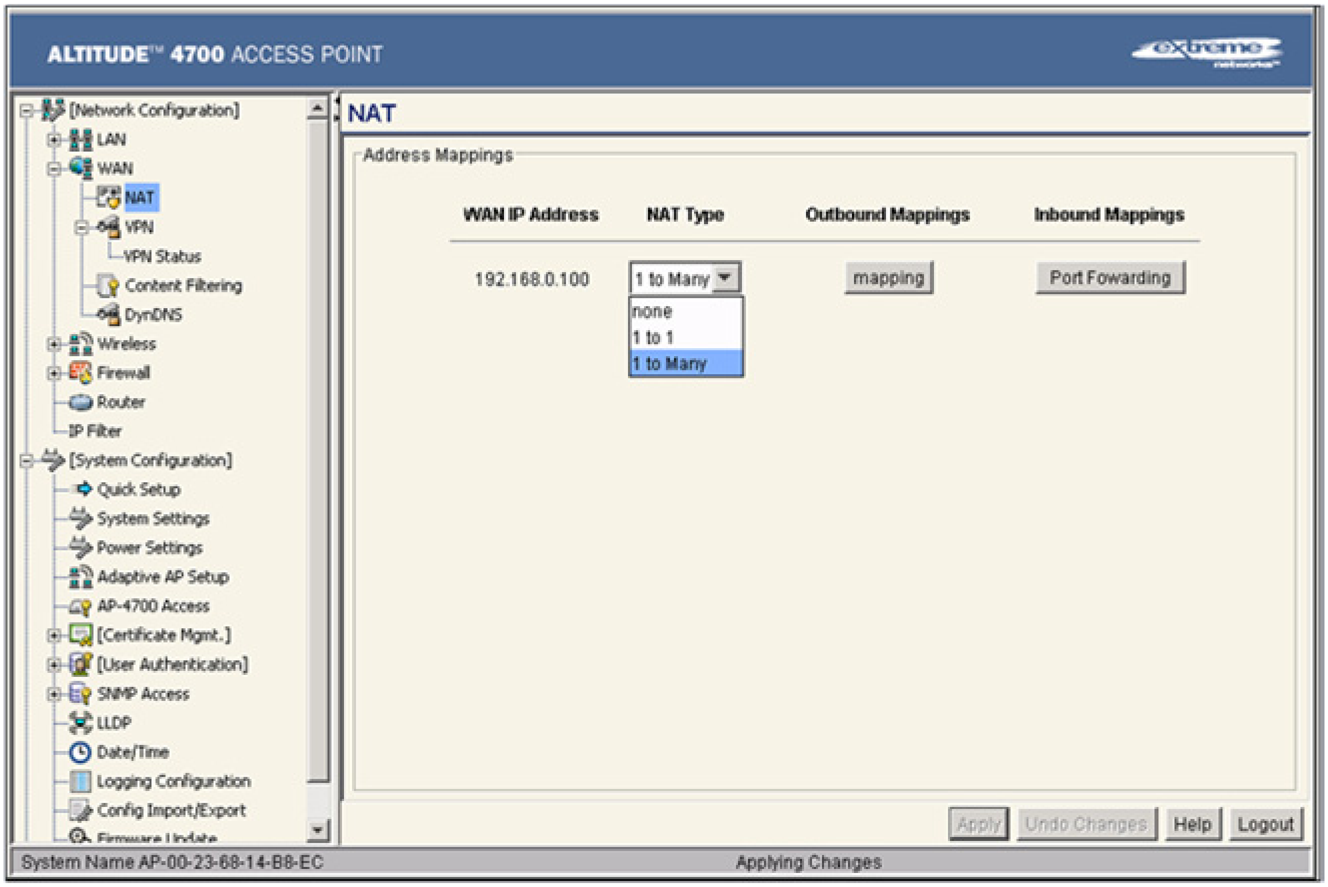
  The private side IP address can belong to any of the private side subnets.

- One-to-many mapping with a configurable range of private side IP addresses

  Ranges can be specified from each of the private side subnets.

To configure IP address mappings for the access point:

1 Select *Network Configuration* > *WAN* > *NAT* from the access point menu tree.



NAT

Address Mappings

WAN IP Address	NAT Type	Outbound Mappings	Inbound Mappings
192.168.0.100	1 to Many	mapping	Port Fowarding

System Name AP-00-23-68-14-B8-EC

Applying Changes

2 Configure the *Address Mappings* field to generate a WAN IP address, define the NAT type and set outbound/inbound NAT mappings.

WAN IP Address

The WAN IP addresses on the NAT screen are dynamically generated from address settings applied on the *WAN* screen.

NAT Type

Specify the NAT Type as *1 to 1* to map a WAN IP address to a single host (local) IP address. 1 to 1 mapping is useful when users need dedicated addresses, and for public-facing servers connected to the access point.

Set the NAT Type as *1 to Many* to map a WAN IP address to multiple local IP addresses. This displays the *mappings* button in the adjacent Outbound Mappings field. This button displays a screen for mapping the LAN IP addresses that are associated with each subnet.

Define the NAT Type as *none* when routable IP addresses are used on the internal network.

Outbound Mappings	When *1 to 1* NAT is selected, a single IP address can be entered in the *Outbound Mappings* area. This address provides a 1 to 1 mapping of the WAN IP address to the specified IP address. When *1 to Many* is selected as the NAT Type, the Outbound Mappings area displays a *1 to Many Mappings* button. Click the button to select the LAN1 or LAN2 IP address used to set the outbound IP address or select *none* to exclude the IP address. If *none* is selected as the NAT Type, the Outbound Mappings area is blank.
Inbound Mappings	When *1 to 1* or *1 to Many* is selected, the *Inbound Mappings* option displays a *Port Forwarding* button.
Port Forwarding	Click the *Port Forwarding* button to display a screen of port forwarding parameters for inbound traffic from the associated WAN IP address. For information on configuring port forwarding, see “Configuring Port Forwarding” on page 143.

3 Click *Apply* to save any changes to the NAT screen. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.

4 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the NAT screen to the last saved configuration.

5 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring Port Forwarding

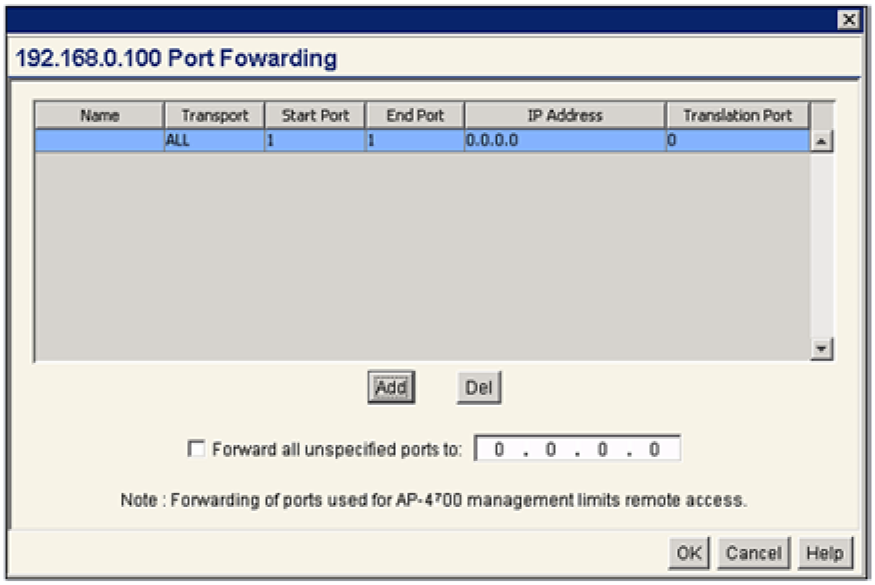
Use the *Port Forwarding* screen to configure port forwarding parameters for inbound traffic from the associated WAN IP address.

To configure port forwarding for the access point:

1 Select *Network Configuration > WAN > NAT* from the access point menu tree.

2 Select *1 to 1* or *1 to Many* from the NAT Type drop-down menu.

3 Click on the *Port Forwarding* button within the *Inbound Mappings* area.



192.168.0.100 Port Fowarding

Name	Transport	Start Port	End Port	IP Address	Translation Port
	ALL	1	1	0.0.0.0	0

□ Forward all unspecified ports to: 0 . 0 . 0 . 0

Note : Forwarding of ports used for AP-4700 management limits remote access.

4 Configure the *Port Forwarding* screen to modify the following:

Add

Click *Add* to create a local map that includes the name, transport protocol, start port, end port, IP address and Translation Port for incoming packets.

Delete

Click *Delete* to remove a selected local map entry.

Name

Enter a name for the service being forwarded. The name can be any alphanumeric string and is used for identification of the service.

Transport

Use the *Transport* pull-down menu to specify the transport protocol used in this service. The choices are *ALL*, *TCP, UDP*, *ICMP*, *AH*, *ESP,* and *GRE.*

Start Port and End Port

Enter the port or ports used by the port forwarding service. To specify a single port, enter the port number in the *Start Port* area. To specify a range of ports, use both the *Start Port* and *End Port* options to enter the port numbers. For example, enter 110 in the Start Port field and 115 in the End Port field.

IP Address

Enter the numerical (non DNS name) IP address to which the specified service is forwarded. This address must be within the specified NAT range for the associated WAN IP address.

Translation Port

Specify the port number used to translate data for the service being forwarded.

Forward all unspecified ports to

Use the *Forward all unspecified ports to* checkbox to enable port forwarding for incoming packets with unspecified ports. In the adjacent area, enter a target forwarding IP address for incoming packets. This number must be within the specified NAT range for the associated WAN IP address.

5 Click *OK* to return to the NAT screen. Within the NAT screen, click *Apply* to save any changes made on the Port Forwarding screen.

6 Click *Cancel* to undo any changes made on Port Forwarding screen. This reverts all settings for the Port Forwarding screen to the last saved configuration.

Configuring Dynamic DNS

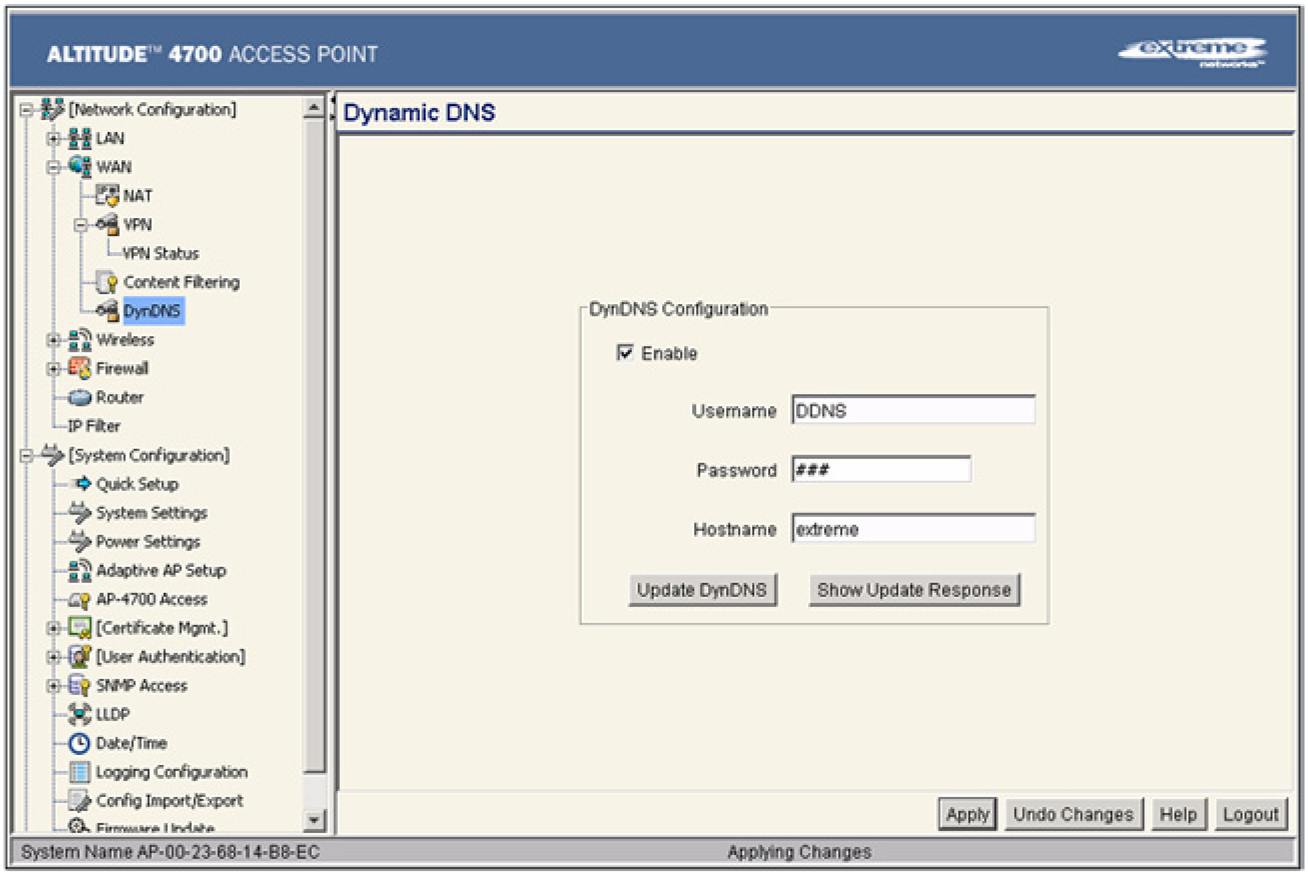
The Access Point supports the Dynamic DNS service. *Dynamic DNS* (or DynDNS) is a feature offered by *www.dyndns.com* which allows the mapping of domain names to dynamically assigned IP addresses via the WAN port. When the dynamically assigned IP address of a client changes, the new IP address is sent to the DynDNS service and traffic for the specified domain(s) is routed to the new IP address.

NOTE

DynDNS supports only the primary WAN IP address.

To configure dynamic DNS for the access point:

1 Select *Network Configuration* > *WAN* > *DynDNS* from the access point menu tree.



DynDNS Configuration

☑ Enable

Username: DDNS

Password: ###

Hostname: extreme

System Name AP-00-23-68-14-B8-EC

Applying Changes

2 Select the *Enable* checkbox to allow domain name information to be updated when the IP address associated with that domain changes.

A username, password and hostname must be specified for domain name information to be updated.

NOTE

The username, password and hostname are required to be registered at http://www.dyndns.com.

3 Enter the DynDNS *Username* for the account you wish to use for the Access Point.

4 Enter the DynDNS *Password* for the account you wish to use for the Access Point.

5 Provide the *Hostname* for the DynDNS account you wish to use for the Access Point.

6 Click the *Update DynDNS* button to update the Access Point's current WAN IP address with the DynDNS service.

NOTE

DynDNS supports devices directly connected to the Internet. Having VPN enabled, and the DynDNS Server on the other side of the VPN is not supported.

7 Once the DynDNS configuration has been updated, click the *Show Update Response* button to open a sub-screen displaying the hostname, IP address and any messages received during an update from the DynDNS Server.

8 Click *Apply* to save any changes to the Dynamic DNS screen. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.

9 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the screen to the last saved configuration.

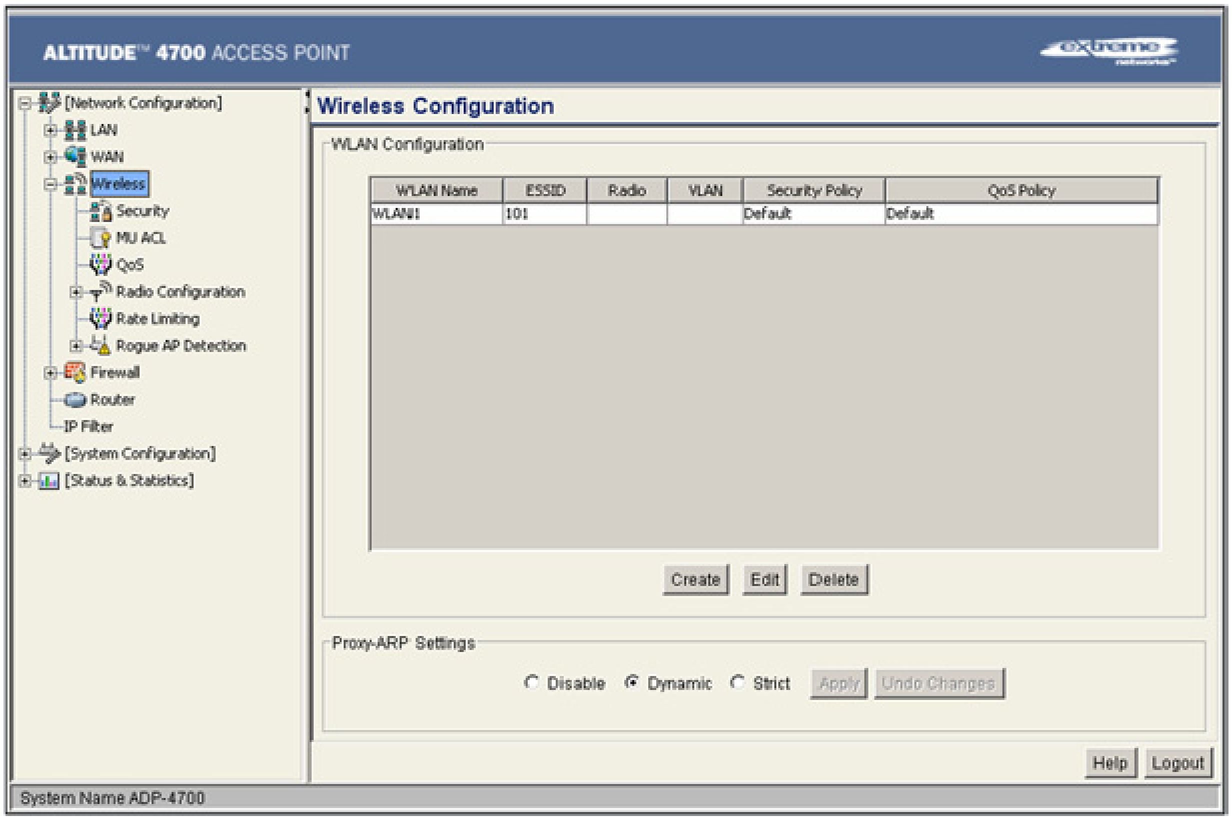
Enabling Wireless LANs (WLANs)

A *Wireless Local Area Network (WLAN)* is a data-communications system that flexibly extends the functionalities of a wired LAN. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable. Within the WLAN, roaming users can be handed off from one access point to another like a cellular phone system. WLANs can therefore be configured around the needs of specific groups of users, even when they are not in physical proximity.

Use the access point's *Wireless Configuration* screen to create new WLANs, edit the properties of existing WLANs or delete a WLAN to create space for a new WLAN. Sixteen WLANs are available on the Access Point (regardless of single or dual-radio model).

To configure WLANs on the access point:

1 Select *Network Configuration* > *Wireless* from the access point menu tree.



Wireless Configuration

WLAN Configuration

WLAN Name	ESSID	Radio	VLAN	Security Policy	QoS Policy
WLAN1	101			Default	Default

Proxy-ARP Settings

○ Disable ● Dynamic ○ Strict

System Name ADP-4700

If a WLAN is defined, that WLAN displays within the Wireless Configuration screen. When the access point is first booted, WLAN1 exists as a default WLAN available immediately for connection.

2 Refer to the information within the Wireless Configuration screen to view the name, ESSID, access point radio designation, VLAN ID and security policy of existing WLANs.

WLAN Name

The *Name* field displays the name of each WLAN that has been defined. The WLAN names can be modified within individual WLAN configuration screens. See "Creating/Editing Individual WLANs" on page 148 to change the name of a WLAN.

ESSID

Displays the *Extended Services Set Identification (ESSID)* associated with each WLAN. The ESSID can be modified within individual WLAN configuration screens. See "Creating/Editing Individual WLANs" on page 148 to change the ESSID of a specific WLAN.

Radio

The *Radio* field displays the name of the access point radio the WLAN is mapped to (either the 802.11a/n radio or the 802.11b/g/n radio). To change the radio designation for a specific WLAN, see "Creating/Editing Individual WLANs" on page 148.

VLAN

The *VLAN* field displays the specific VLAN the target WLAN is mapped to. For information on VLAN configuration for the WLAN, see "Configuring VLAN Support" on page 126.

Security Policy	The *Security Policy* field displays the security profile configured for the target WLAN. For information on configuring security for a WLAN,
QoS Policy	The *QoS Policy* field displays the quality of service currently defined for the WLAN. This policy outlines which data types receive priority for the user base comprising the WLAN. For information on QoS configuration for the WLAN, see "Setting the WLAN Quality of Service (QoS) Policy" on page 156.

3 Click the *Create* button (if necessary) to launch the *New WLAN* screen. Use the New WLAN screen to define the properties of a new WLAN that would display and be selectable within the *Wireless Configuration* screen. For additional information, see "Creating/Editing Individual WLANs" on page 148.

4 Click the *Edit* button (if necessary) to launch the *Edit WLAN* screen. Use the Edit WLAN screen to revise the properties of an existing WLAN that would continue display and be selectable within the *Wireless Configuration* screen. For additional information, see "Creating/Editing Individual WLANs" on page 148.

5 Consider using the *Delete* button to remove an existing WLAN if it has become outdated and is no longer required or if you are coming close the maximum 16 WLANs available per access point.

6 Refer to the *Proxy-ARP Disable* field to enable/disable Proxy AP support. Proxy ARP is disabled by default.

When enabled, any system on the wireless network that ARPs for the IP address of an associated MU receives an ARP reply from the Access Point stating the requesting system should be sending packets destined for the MU to Access Point instead. In turn, the Access Point forwards the requesting packets to the target MU. Through this process, the Access Point can pass ARP requests in both directions, making an MU appear to be connected to a public network even though it's on a private network, hidden behind the Access Point.

Select the following options as required:

a Select *Dynamic* for the Access Point to respond to an ARP request for its MU IP addresses using an ARP response and drop the original ARP request packet.

b Select *Strict* for the Access Point to respond to ARP request for its MU IP addresses using an ARP response and drop the original ARP request packet (like the dynamic option). However, with the strict option, the Access Point will drop the ARP request to wireless (WLAN interfaces not the mesh interface) if the ARP request is for the IP address of non-MUs or if gratuitous ARP requests are coming from the MU. This helps reduce unnecessary ARP traffic and improve throughput within the Access Point managed wireless network.

7 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Creating/Editing Individual WLANs

If the WLANs displayed within the *Wireless Configuration* screen do not satisfy your network requirements, you can either create a new WLAN or edit the properties of an existing WLAN.

NOTE

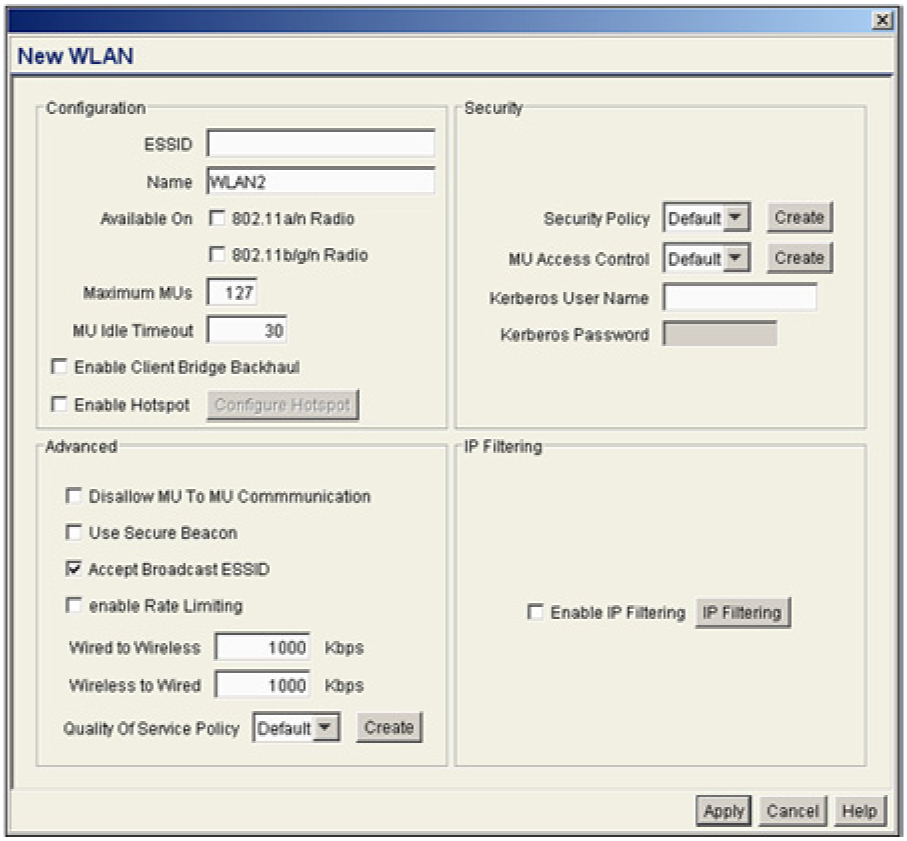
Before editing the properties of an existing WLAN, ensure it is not being used by an access point radio, or is a WLAN that is needed in its current configuration. Once updated, the previous configuration is not available unless saved.

Use the New WLAN and Edit WLAN screens as required to create/modify a WLAN. To create a new WLAN or edit the properties of an existing WLAN:

1 Select *Network Configuration* > *Wireless* from the access point menu tree.

The Wireless Configuration screen displays.

2 Click the *Create* button to configure a new WLAN, or highlight a WLAN and click the *Edit* button to modify an existing WLAN. Either the *New WLAN* or *Edit WLAN* screen displays.



New WLAN

Configuration

ESSID

Name: WLAN2

Available On: □ 802.11a/n Radio □ 802.11b/g/n Radio

Maximum MUs: 127

MU Idle Timeout: 30

□ Enable Client Bridge Backhaul

□ Enable Hotspot

Security

Security Policy: Default

MU Access Control: Default

Kerberos User Name

Kerberos Password

Advanced

□ Disallow MU To MU Commmunication

□ Use Secure Beacon

☑ Accept Broadcast ESSID

□ enable Rate Limiting

Wired to Wireless: 1000 Kbps

Wireless to Wired: 1000 Kbps

Quality Of Service Policy: Default

IP Filtering

□ Enable IP Filtering

3 Set the parameters in the *Configuration* field as required for the WLAN.

CAUTION

When using the Access Point’s hotspot functionality, ensure MUs are re-authenticated when changes are made to the characteristics of a hotspot enabled WLAN, as MUs within the WLAN will be dropped from device association.

ESSID

Enter the *Extended Services Set Identification (ESSID)* associated with the WLAN. The WLAN name is auto-generated using the ESSID until changed by the user. The maximum number of characters that can be used for the ESSID is 32. Do not use any of the following characters for an ESSID < > | " & \ ? ,

Name

Define or revise the name for the WLAN. The name should be logical representation of WLAN coverage area (engineering, marketing etc.). The maximum number of characters that can be used for the name is 31.

Available On

Use the *Available On* checkboxes to define whether the WLAN you are creating or editing is available to clients on either the 802.11a/n or 802.11b/g/n radio (or both radios). The Available On checkbox should only be selected for a mesh WLAN if this target Access Point is to be configured as a base bridge or repeater (base and client bridge) on the radio. If the radio for the WLAN is to be defined as a client bridge only, the Available On checkbox should not be selected**.** For more information on defining a WLAN for mesh support, see "Configuring a WLAN for Mesh Networking Support" on page 583.

Max MUs

Use the *Max MUs* field to define the number of MUs permitted to interoperate within the new or revised WLAN. The maximum (and default) is 127. However, each Access Point can only support a maximum 127 MUs spanned across its 16 available WLANs. If you intend to define numerous WLANs, ensure each is using a portion of the 127 available MUs and the sum of the supported MUs across all WLANs does not exceed 127.

MU Idle Timeout

Set an *MU Idle Timeout* the Access Point uses to timeout idle mobile units from WLAN inclusion. When exceeded, the MU must re-establish its credentials to assume operation within the WLAN. Set a value between 1–65535 minutes. the default value is 30 minutes.

Enable Client Bridge Backhaul

Select the Enable *Client Bridge Backhaul* checkbox to make the WLAN available in the *WLAN* drop-down menu within the *Radio Configuration* screen. This checkbox can be ignored for WLANs not supporting mesh networking, to purposely exclude them from the list of WLANs available in the Radio Configuration page selected specifically for mesh networking support. Only WLANs defined for mesh networking support should have this checkbox selected.

Enable Hotspot

Select the *Enable Hotspot* checkbox to allow this WLAN (whether it be a new or existing WLAN) to be configured for hotspot support. Clicking the *Configure Hotspot* button launches a screen wherein the parameters of the hotspot can be defined. For information on configuring a target WLAN for hotspot support, see "Configuring WLAN Hotspot Support" on page 160. For an overview of what a hotspot is and what it can provide your wireless network,

CAUTION

A WLAN cannot be enabled for both mesh and hotspot support at the same time. Only one of these two options can be enabled at one time, as the GUI and CLI will prevent both from being enabled.

NOTE

If 802.11a/n is selected as the radio used for the WLAN, the WLAN cannot use a Kerberos supported security policy.

4 Configure the *Security* field as required to set the data protection requirements for the WLAN.

NOTE

A WLAN configured to support Mesh should not have a Kerberos or 802.1x EAP security policy defined for it, as these two authentication schemes are not supported within a Mesh network.

Security Policy

Use the scroll down *Security Policies* menu to select the security scheme best suited for the new or revised WLAN. Click the *Create* button to jump to the New Security Policy screen where a new policy can be created to suit the needs of the WLAN. For more information, see "Configuring WLAN Security Policies" on page 152**.**

MU Access Control

Select an ACL policy suiting the WLAN's MU interoperability requirements from the drop-down menu. If the existing ACL policies do not satisfy the requirements of the WLAN, a new ACL policy can be created by pressing the *Create* button. For more information, see "Configuring a WLAN Access Control List (ACL)" on page 153.

Kerberos User Name

Displays the read-only Kerberos User Name used to associate the wireless client. This value is the ESSID of the Access Point.

Kerberos Password

Enter a Kerberos password if *Kerberos* has been selected as the security scheme from within the *Security Policies* field. The field is grayed out if Kerberos has not been selected for the WLAN. For information on configuring Kerberos,

5 Configure the *Advanced* field as required to set MU interoperability permissions, secure beacon transmissions, broadcast ESSID acceptance and *Quality of Service (QoS)* policies.

Disallow MU to MU Communication

The MU-MU Disallow feature prohibits MUs from communicating with each other even if they are on different WLANs, assuming one of the WLAN's is configured to disallow MU-MU communication. Therefore, if an MU's WLAN is configured for MU-MU disallow, it will not be able to communicate with any other MUs connected to this Access Point.

Use Secure Beacon

Select the *Use Secure Beacon* checkbox to not transmit the Access Point's ESSID. If a hacker tries to find an ESSID via an MU, the ESSID does not display since the ESSID is not in the beacon. Extreme Networks recommends keeping the option enabled to reduce the likelihood of hacking into the WLAN.

Accept Broadcast ESSID

Select the *Accept Broadcast ESSID* checkbox to associate an MU that has a blank ESSID (regardless of which ESSID the Access Point is currently using). Sites with heightened security requirements may want to leave the checkbox unselected and configure each MU with an ESSID. The default is selected.

Enable Rate Limiting	Select this checkbox to set MU rate limiting values for this WLAN in both the upstream and downstream direction. Once selected, two fields display enabling you to set MU radio bandwidth for each associated MU in both the wired-to-wireless and wireless-to-wired directions. Set an allocation between 100 and 300,000 kbps. The default value is 1000 kbps. For more information, see "Configuring MU Rate Limiting" on page 184.
Quality of Service Policy	If QoS policies are undefined (none), select the *Create* button to launch the *New QoS Policy* screen. Use this screen to create a QoS policy, wherein data traffic for the new or revised WLAN can be prioritized to best suit the MU transmissions within that WLAN. For more information, see "Setting the WLAN Quality of Service (QoS) Policy" on page 156.

6 Refer to the *IP Filtering* field to optionally enable the IP filtering feature, and (if enabled) apply existing IP filters (and their rules and permissions) to the WLAN.

Enable IP Filtering	Selecting this checkbox allows the WLAN to employ filter policies and rules to determine which IP packets are processed normally over the WLAN and which are discarded. If discarded, a packet is deleted and ignored (as if never received).
IP Filtering	Select the IP Filtering button to display a screen where existing IP filter policies can be applied to the WLAN to allow or deny IP packets in either an incoming or outgoing direction based on the rules defined for the policy.

NOTE

For an overview of IP Filtering and how to create a filter, see "Configuring IP Filtering" on page 188. For information on applying an existing filter to the IP packet flow of a WLAN, see "Applying a Filter to LAN1, LAN2 or a WLAN (1-16)" on page 191.

7 Click *Apply* to save any changes to the WLAN screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

8 Click *Cancel* to securely exit the New WLAN or Edit WLAN screen and return to the Wireless Configuration screen.

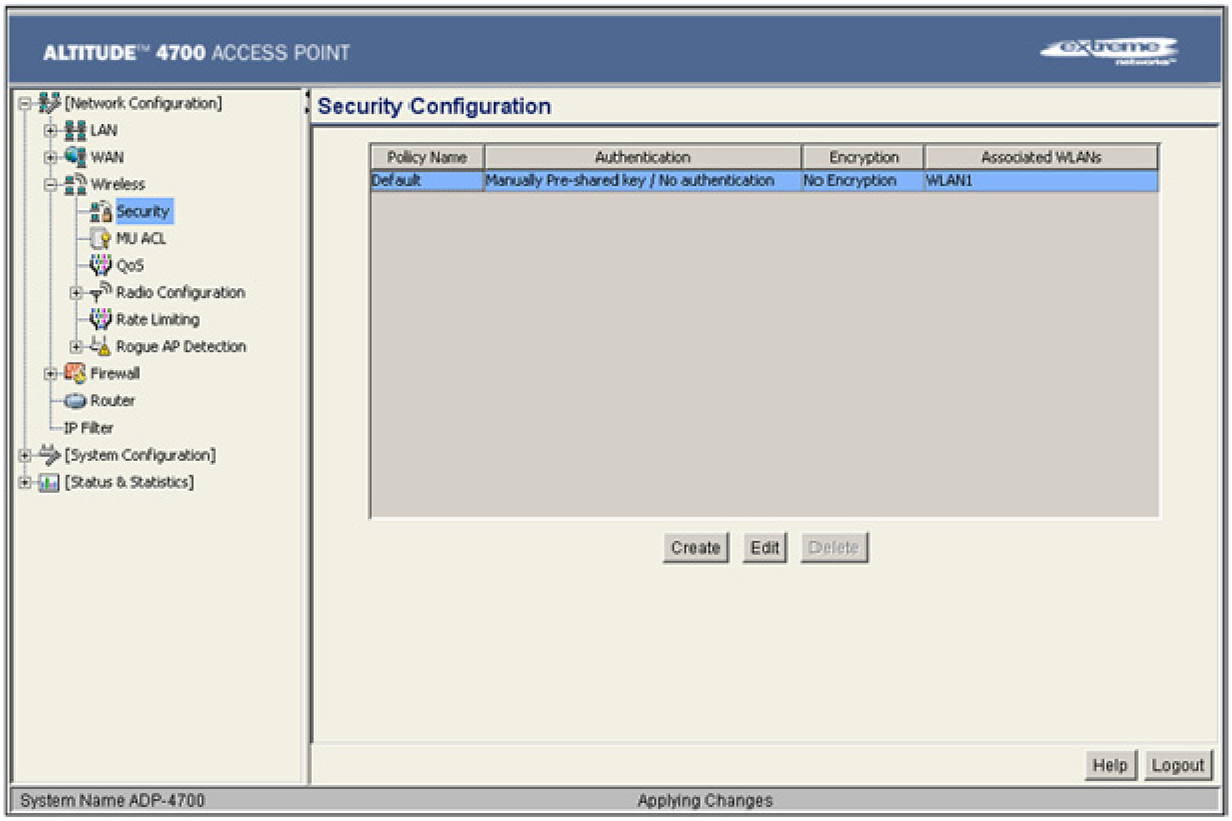
Configuring WLAN Security Policies

As WLANs are being defined for an access point, a security policy can be created or an existing policy edited (using the *Create* or *Edit* buttons within the *Security Configuration* screen) to best serve the security requirements of the WLAN. Once new policies are defined, they are available within the *New WLAN* or *Edit WLAN* screens and can be mapped to any WLAN. A single security policy can be used by more than one WLAN if its logical to do so. For example, there may be two or more WLANs within close proximity of each other requiring the same data protection scheme.

To create a new security policy or modify an existing policy:

1 Select *Network Configuration* > *Wireless* > *Security* from the access point menu tree.

The *Security Configuration* screen appears with existing policies and their attributes displayed.



Policy Name	Authentication	Encryption	Associated WLANs
Default	Manually Pre-shared key / No authentication	No Encryption	WLAN1

System Name ADP-4700

Applying Changes

NOTE

When the access point is first launched, a single security policy (default) is available and mapped to WLAN 1. It is anticipated numerous additional security policies will be created as the list of WLANs grows.

Configuring a WLAN security scheme with a discussion of all the authentication and encryption options available is beyond the scope of this chapter. See “Configuring Access Point Security” on page 197 for more details on configuring access point security.

For detailed information on the authentication and encryption options available to the access point and how to configure them, see to “Configuring Security Options” on page 197 and locate the section that describes your intended security scheme.

2 Click *Logout* to exit the Security Configuration screen.

Configuring a WLAN Access Control List (ACL)

An *Access Control List (ACL)* affords a system administrator the ability to grant or restrict MU access by specifying an MU MAC address or range of MAC addresses to either include or exclude from access point connectivity. Use the *Mobile Unit Access Control List Configuration* screen to create new ACL policies (using the *New MU ACL Policy* sub-screen) or edit existing policies (using the *Edit MU ACL Policy* sub-screen). Once new policies are defined, they are available for use within the *New WLAN* or *Edit WLAN* screens to assign to specific WLANs based on MU interoperability requirements.

Extreme Networks recommends using the New MU ACL Policy or Edit MU ACL Policy screens strategically to name and configure ACL policies meeting the requirements of the particular WLANs they may map to. However, be careful not to name policies after specific WLANs, as individual ACL policies can be used by more than one WLAN. For detailed information on assigning ACL policies to specific WLANs, see "Creating/Editing Individual WLANs" on page 148.

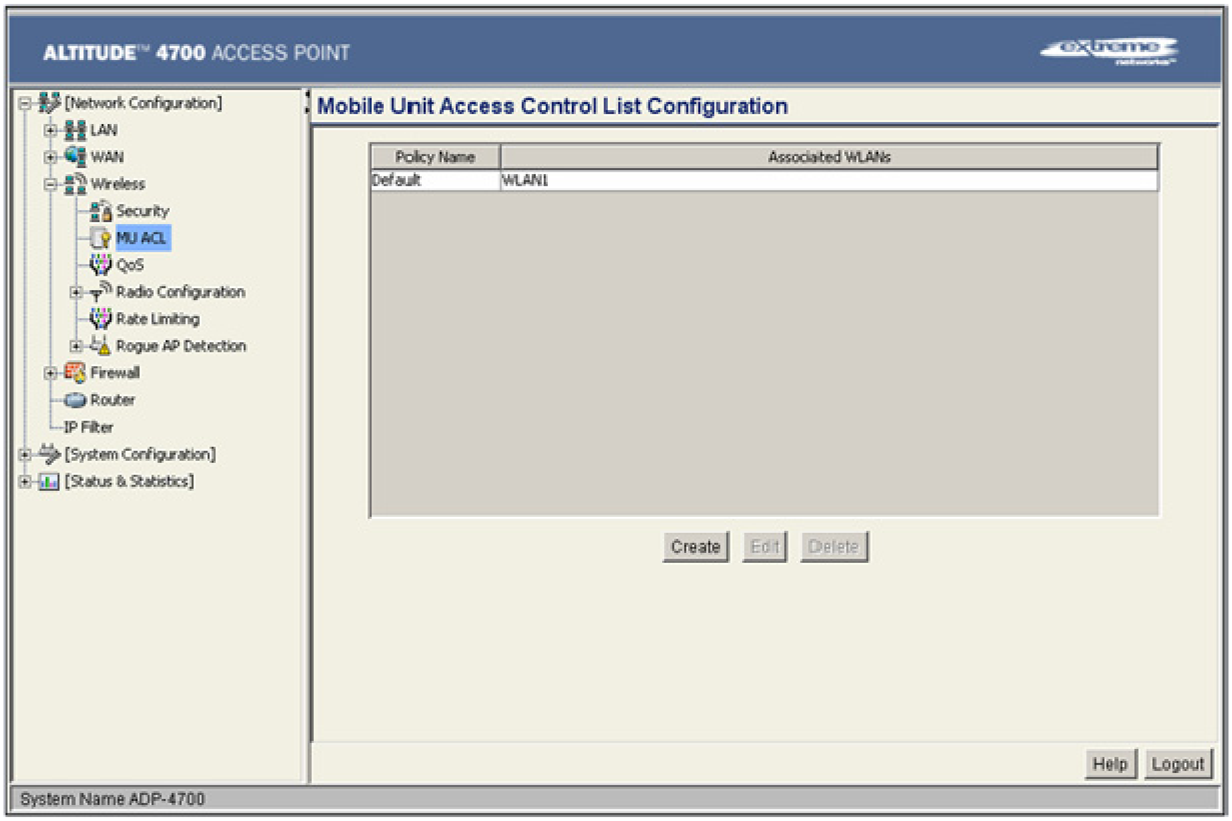
To create or edit ACL policies for WLANs:

1 Select *Network Configuration* > *Wireless* > *MU ACL* from the access point menu tree.

The *Mobile Unit Access Control List Configuration* screen displays with existing ACL policies and their current WLAN (if mapped to a WLAN).

NOTE

When the access point is first launched, a single ACL policy (default) is available and mapped to WLAN 1. It is anticipated numerous additional ACL policies will be created as the list of WLANs grows.

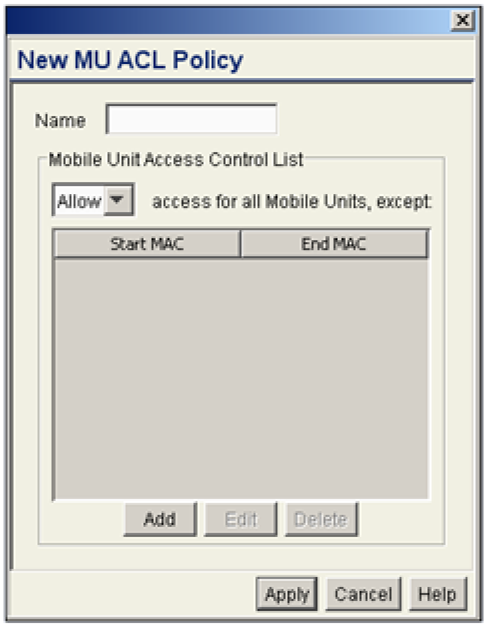


Mobile Unit Access Control List Configuration

Policy Name	Associated WLANs
Default	WLAN1

System Name ADP-4700

2 Click the *Create* button to configure a new ACL policy, or select a policy and click the *Edit* button to modify an existing ACL policy. The Access Point supports a maximum of 16 MU ACL policies.



Either the *New MU ACL Policy* or *Edit MU ACL Policy* screen displays.

3 Assign a name to the new or edited ACL policy that represents an inclusion or exclusion policy specific to a particular type of MU traffic you may want to use with a single or group of WLANs. More than one WLAN can use the same ACL policy.

4 Configure the parameters within the *Mobile Unit Access Control List* field to allow or deny MU access to the access point.

The MU adoption list identifies MUs by their MAC address. The MAC address is the MU's unique *Media Access Control* number printed on the device (for example, 00:09:5B:45:9B:07) by the manufacturer. A maximum of 200 MU MAC addresses can be added to the New/Edit MU ACL Policy screen.

Access for the listed Mobile Units	Use the drop-down list to select *Allow* or *Deny*. This rule applies to the MUs listed in the table. For example, if the adoption rule is to Allow, access is granted for all MUs except those listed in the table.
Add	Click the *Add* button to create a new entry using only the *Start MAC* column to specify a MAC address, or uses both the *Start MAC* and *End MAC* columns to specify a range of MAC addresses.
Delete	Click the *Delete* button to remove a selected list entry.

5 Click *Apply* to save any changes to the New MU ACL Policy or Edit MU ACL Policy screen and return to the Mobile Unit Access Control List Configuration screen. Navigating away from the screen without clicking Apply results in changes to the screens being lost.

6 Click *Cancel* to securely exit the New MU ACL Policy or Edit MU ACL Policy screen and return to the Mobile Unit Access Control List Configuration screen.

7 Click *Logout* within the Mobile Unit Access Control List Configuration screen to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Setting the WLAN Quality of Service (QoS) Policy

The access point can keep a list of QoS policies that can be used from the *New WLAN* or *Edit WLAN* screens to map to individual WLANs. Use the *Quality of Service Configuration* screen to configure WMM policies that can improve the user experience for audio, video and voice applications by shortening the time between packet transmissions for higher priority (multimedia) traffic.

Use the *Quality of Service Configuration* screen to define the QoS policies for advanced network traffic management and multimedia applications support. If the existing QoS policies are insufficient, a new policy can be created or an existing policy can be modified using the *New QoS Policy* or *Edit QoS Policy* screens. Once new policies are defined, they are available for use within the *New WLAN* or *Edit WLAN* screens to assign to specific WLANs based on MU interoperability requirements.

Extreme Networks recommends using the New QoS Policy and Edit QoS Policy screens strategically to name and configure QoS policies meeting the requirements of the particular WLANs they may belong to. However, be careful not to name policies after specific WLANs, as individual QoS policies can be used by more than one WLAN. For detailed information on assigning QoS policies to specific WLANs, see "Creating/Editing Individual WLANs" on page 148.

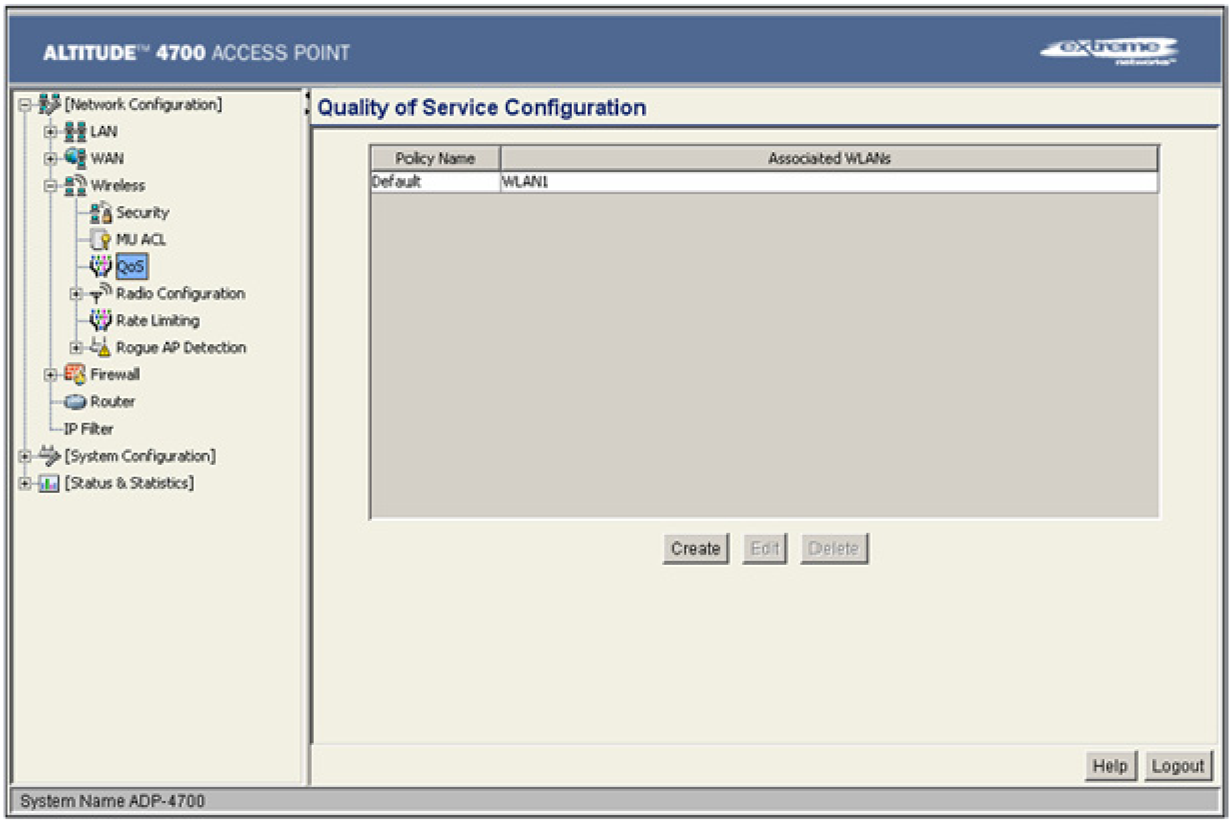
To configure QoS policies:

1 Select *Network Configuration* > *Wireless* > *QoS* from the access point menu tree.

The *Quality of Service Configuration* screen displays with existing QoS policies and their current WLAN (if mapped to a WLAN).

NOTE

When the access point is first launched, a single QoS policy (default) is available and mapped to WLAN 1. It is anticipated additional QoS policies will be created as the list of WLANs grows.

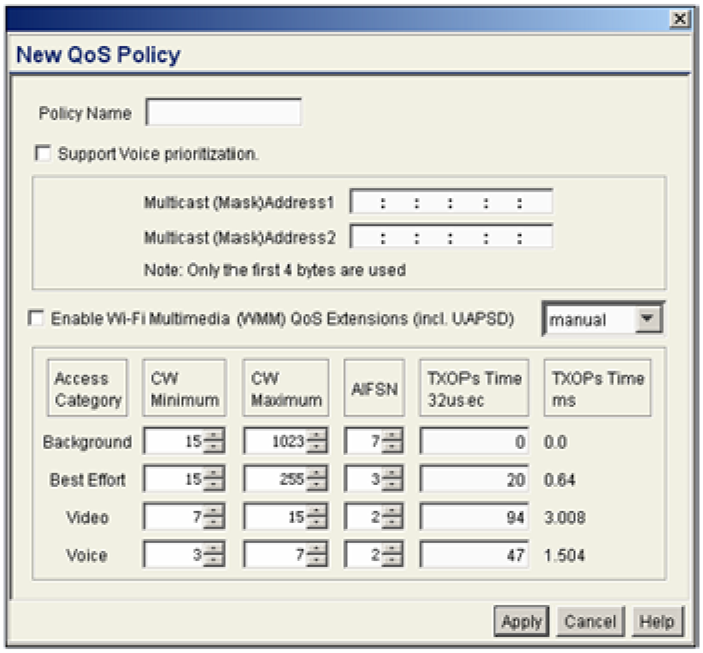


Quality of Service Configuration

Policy Name	Associated WLANs
Default	WLAN1

System Name ADP-4700

2 Click the *Create* button to configure a new QoS policy, or select a policy and click the *Edit* button to modify an existing QoS policy. The Access Point supports a maximum of 16 QoS policies.



New QoS Policy

Policy Name

□ Support Voice prioritization.

Multicast (Mask)Address1 : : : : :

Multicast (Mask)Address2 : : : : :

Note: Only the first 4 bytes are used

□ Enable Wi-Fi Multimedia (WMM) QoS Extensions (incl. UAPSD) manual

Access Category	CW Minimum	CW Maximum	AIFSN	TXOPs Time 32usec	TXOPs Time ms
Background	15	1023	7	0	0.0
Best Effort	15	255	3	20	0.64
Video	7	15	2	94	3.008
Voice	3	7	2	47	1.504

3 Assign a name to the new or edited QoS policy that makes sense to the access point traffic receiving priority. More than one WLAN can use the same QoS policy.

4 Select the *Support Voice prioritization* checkbox to allow legacy voice prioritization.

Certain products may not receive priority over other voice or data traffic. Consequently, ensure the *Support Voice Prioritization* checkbox is selected if using products that do not support Wi-Fi Multimedia (WMM) to provide preferred queuing for these VOIP products.

If the *Support Voice Prioritization* checkbox is selected, the Access Point will detect non-WMM capable (legacy) phones that connect to the Access Point and provide priority queueing for their traffic over normal data.

NOTE

Wi-fi functionality requires both the Access Point and its associated clients are WMM-capable and have WMM enabled. WMM enabled devices can take advantage of their QoS functionality only if using applications that support WMM, and can assign an appropriate priority level to the traffic streams they generate.

5 Use the two *Multicast Address* fields to specify one or two MAC addresses used for multicast applications. Some VoIP devices make use of multicast addresses. Using this mechanism ensures multicast packets for these devices are not delayed by the packet queue. Only the first four bytes are used.

6 Use the drop-down menu to select the radio traffic best representing the network requirements of this WLAN. Options include:

manual	Select the *manual* option if intending to manually set the Access Categories for the radio traffic within this WLAN. Only advanced users should manually configure the Access Categories, as setting them inappropriately could negatively impact the Access Point's performance.
11ag - wifi	Use this setting for high-end multimedia devices that using the high rate 802.11a or 802.11g radio.
11b - wifi	Use this setting for high-end devices multimedia devices that use the 802.11b radio.
11ag - default	Use this setting for typical “data-centric” MU traffic over the high rate 802.11a or 802.11g radio.
11b - default	Use this setting for typical “data-centric” MU traffic over the 802.11b radio.
11ag voice	Use this setting for “Voice-Over-IP” traffic over the high rate 802.11a or 802.11g radio.
11b voice	Use this setting for “Voice-Over-IP” traffic over the 802.11b radio.

CAUTION

Extreme Networks recommends using the drop-down menu to define the intended radio traffic within the WLAN. Once an option is selected, you do not need to adjust the values for the Access Categories, unless qualified to do so. Changing the Access Category default values could negatively impact the performance of the Access Point.

7 Select the *Enable Wi-Fi Multimedia (WMM) QoS Extensions* checkbox to configure the access point's QoS Access Categories. The Access Categories are not configurable unless the checkbox is selected. Access Categories include:

Background	Background traffic is typically of a low priority (file transfers, print jobs ect.). Background traffic typically does not have strict latency (arrival) and throughput requirements.
Best Effort	Best Effort traffic includes traffic from legacy devices or applications lacking QoS capabilities. Best Effort traffic is negatively impacted by data transfers with long delays as well as multimedia traffic.
Video	Video traffic includes music streaming and application traffic requiring priority over all other types of network traffic.
Voice	Voice traffic includes VoIP traffic and typically receives priority over Background and Best Effort traffic.

8 Configure the *CW min* and *CW max* (contention windows), *AIFSN* (*Arbitrary Inter-Frame Space Number*) and *TXOPs Time* (opportunity to transmit) for each Access Category. Their values are explained as follows.

CW Min	The contention window minimum value is the least amount of time the MU waits before transmitting when there is no other data traffic on the network. The longer the interval, the lesser likelihood of collision. This value should be set to a smaller increment for higher priority traffic. Reduce the value when traffic on the WLAN is anticipated as being smaller.
CW Max	The contention window maximum value is the maximum amount of time the MU waits before transmitting when there is no other data traffic on the network. The longer the interval, the lesser likelihood of collision, but the greater propensity for longer transmit periods.
AIFSN	The AIFSN is the minimum interframe space between data packets transmitted for the selected Access Category. This value should be set to a smaller increment for higher priority traffic to reduce packet delay time.
TXOPs Time 32usec	The *TXOPs Time* is the interval the transmitting MU is assigned for transmitting. The default for Background traffic is 0. The same TXOPs values should be used for either the 802.11a/n or 802.11b/g/n radio, there is no difference.
TXOPs Time ms	TXOP times range from 0.2 ms (background priority) to 3 ms (video priority) in a 802.11a/n network, and from 1.2 ms to 6 ms in an 802.11b/g/n network. The TXOP bursting capability greatly enhances the efficiency for high rate traffic such as streaming video.

9 Click *Apply* to save any changes to the New QoS Policy or Edit QoS Policy screen to return to the Quality of Service Configuration screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

10 Click *Cancel* to securely exit the New QoS Policy or Edit QoS Policy screen and return to the Quality of Service Configuration screen.

11 Click *Logout* within the Quality of Service Configuration screen to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

U-APSD (WMM Power Save) Support

The Access Point now supports *Unscheduled Automatic Power Save Delivery* (U-APSD), often referred to as WMM Power Save. U-APSD provides a periodic frame exchange between a voice capable MU and the Access Point during a VoIP call, while legacy power management is still utilized for typical data frame exchanges. The Access Point and its associated MU activate the new U-APSD power save approach when a VoIP traffic stream is detected. The MU then buffers frames from the voice traffic stream and sends a VoIP frame with an implicit “poll” request to its associated Access Point. The Access Point responds to the poll request with buffered VoIP stream frame(s). When a voice-enabled MU wakes up at a designated VoIP frame interval, it sends a VoIP frame with an implicit “poll” request to its associated Access Point. The Access Point responds to the poll request with buffered VoIP stream frame(s).

NOTE

The Access Point ships with the U-APSD feature disabled by default. It is automatically enabled when WMM is enabled for a WLAN. Thus, U-APSD is only functional when WMM is enabled. If WMM is disabled, then U-APSD is disabled as well.

Configuring WLAN Hotspot Support

The Access Point enables hotspot operators to provide user authentication and accounting without a special client application. The Access Point uses a traditional Internet browser as a secure authentication device. Rather than rely on built-in 802.11 security features to control Access Point association privileges, configure a WLAN with no WEP (an open network). The Access Point issues an IP address to the user using a DHCP server, authenticates the user and grants the user to access the Internet.

When a user visits a public hotspot and wants to browse to a Web page, they boot up their laptop and associate with the local Wi-Fi network by entering the correct SSID. They then start a browser. The hotspot access controller forces this un-authenticated user to a Welcome page from the hotspot Operator that allows the user to login with a username and password.

NOTE

Beginning with this most recent 4.1 release of the Access Point firmware, users now have the ability to customize the appearance of an Access Point’s hotspot pages. The Access Point’s hotspot feature is supported by three customer accessible pages (login page, welcome page and failure page) displayed on the client attempting to access the AP’s supported hotspot. These three pages can be unique to each hotspot supported by one of the Access Point’s 16 WLANs. For more information, see “Customizing a Hotspot Display” on page 165.

The Access Point hotspot functionality requires the following:

- *HTTP Redirection*—Redirects unauthenticated users to a specific page specified by the Hotspot provider.
- *User authentication*—Authenticates users using a RADIUS server.
- *Walled garden support*—Enables a list of IP address (not domain names) accessed without authentication.
- *Billing system integration*—Sends accounting records to a RADIUS accounting server.

CAUTION

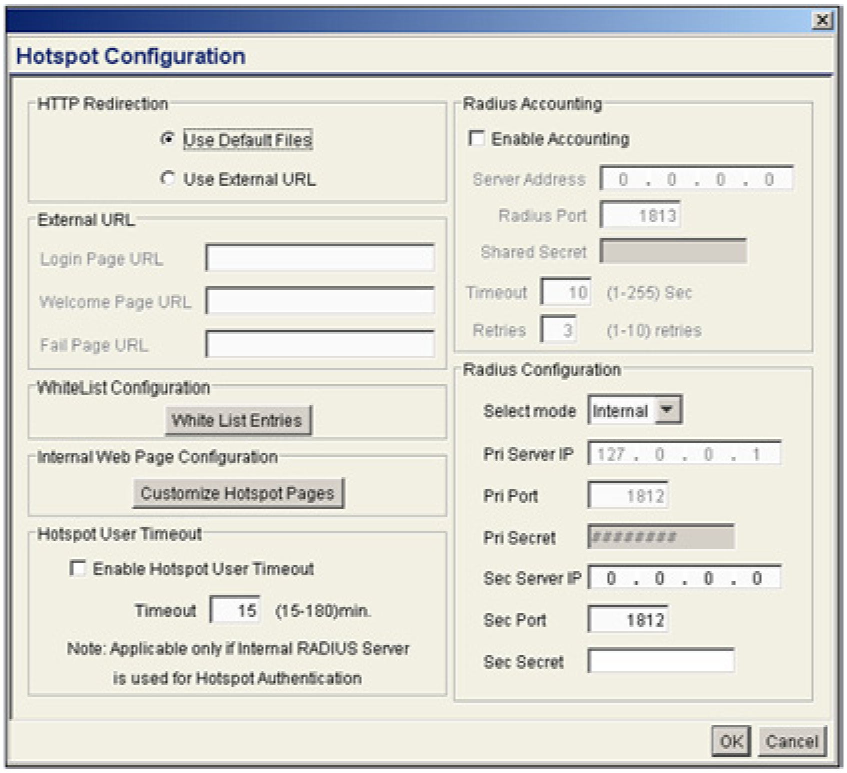
When using the Access Point's hotspot functionality, ensure MUs are re-authenticated when changes are made to the characteristics of a hotspot enabled WLAN, as MUs within the WLAN will be dropped from Access Point device association.

To configure hotspot functionality for an Access Point WLAN:

1 Ensure the *Enable Hotspot* checkbox is selected from within the target WLAN screen, and ensure the WLAN is properly configured.

Any of the sixteen WLANs on the Access Point can be configured as a hotspot. For hotspot enabled WLANs, DHCP, DNS, HTTP and HTTPS traffic is allowed (before you login to the hotspot), while TCP/IP packets are redirected to the port on the subnet to which the WLAN is mapped. For WLANs not hotspot-enabled, all packets are allowed.

2 Click the *Configure Hotspot* button within the WLAN screen to display the *Hotspot Configuration* screen for that target WLAN.



Hotspot Configuration

HTTP Redirection
● Use Default Files
○ Use External URL

External URL
Login Page URL
Welcome Page URL
Fail Page URL

WhiteList Configuration
White List Entries

Internal Web Page Configuration
Customize Hotspot Pages

Hotspot User Timeout
□ Enable Hotspot User Timeout
Timeout 15 (15-180)min.
Note: Applicable only if Internal RADIUS Server is used for Hotspot Authentication

Radius Accounting
□ Enable Accounting
Server Address 0 . 0 . 0 . 0
Radius Port 1813
Shared Secret
Timeout 10 (1-255) Sec
Retries 3 (1-10) retries

Radius Configuration
Select mode Internal
Pri Server IP 127 . 0 . 0 . 1
Pri Port 1812
Pri Secret ########
Sec Server IP 0 . 0 . 0 . 0
Sec Port 1812
Sec Secret

OK Cancel

3 Refer to the *HTTP Redirection* field to specify how the Login, Welcome, and Fail pages are maintained for this specific WLAN. The pages can be hosted locally or remotely.

Use Default Files

Select the *Use Default Files* checkbox if the login, welcome and fail pages reside on the Access Point.

Use External URL — Select the *Use External URL* checkbox to define a set of external URLs for hotspot users to access the login, welcome and fail pages. To create a redirected page, you need to have a TCP termination locally. On receiving the user credentials from the login page, the Access Point connects to a RADIUS server, determines the identity of the connected wireless user and allows the user to access the Internet based on successful authentication.

4 Use the *External URL* field to specify the location of the login page, welcome page and fail page used for hotspot access. Defining these settings is required when the *Use External URL* checkbox has been selected within the HTTP Redirection field.

NOTE

If an external URL is used, the external Web pages are required to forward user credentials to the Access Point, which in turn forwards them to the authentication Server (either onboard or external server) in order to grant users Web access.

Login Page URL — Define the complete URL for the location of the Login page. The Login screen will prompt the hotspot user for a username and password to access the Welcome page.

Welcome Page URL — Define the complete URL for the location of the Welcome page. The Welcome page asserts the hotspot user has logged in successfully and can access the Internet.

Fail Page URL — Define the complete URL for the location of the Fail page. The Fail screen asserts the hotspot authentication attempt failed, you are not allowed to access the Internet and you need to provide correct login information to access the Internet.

5 Select the *Enable Hotspot User Timeout* checkbox to define a timeout interval forcing users (when exceeded) to re-establish their login credentials to continue using the Access Point supported hotspot.

Leaving the checkbox unselected is not recommended unless you plan to provide unlimited hotspot support to users.

If this option is selected, enter an interval (between 15 and 180 minutes). When the provided interval is exceeded, the user is logged out of their hotspot session and forced to login to the hotspot again to access to the hotspot supported WLAN. The default timeout interval is 15 minutes.

NOTE

The Enable Hotspot User Timeout option is only available if using the Access Point's internal RADIUS Server for user authentication.

6 Click the *White List Entries* button (within the *WhiteList Configuration* field) to create a set of allowed destination IP addresses. These allowed destination IP addresses are called a White List. Ten configurable IP addresses are allowed for each WLAN. For more information, see "Defining the Hotspot White List" on page 164.

NOTE

If using an external Web Server over the WAN port, and the hotspot’s HTTP pages (login or welcome) redirect to the Access Point’s WAN IP address for CGI scripts, the IP address of the external Web server and the Access Point’s WAN IP address should be entered in the White List.

7 Refer to the *Radius Accounting* field to enable RADIUS accounting and specify the a timeout and retry value for the RADIUS server.

Enable Accounting — Select the *Enable Accounting* checkbox to enable a RADIUS Accounting Server used for RADIUS authentication for a target hotspot user.

Server Address — Specify an IP address for the external RADIUS Accounting server used to provide RADIUS accounting for the hotspot. If using this option, an internal RADIUS server cannot be used. The IP address of the internal RADIUS server is fixed at 127.0.0.1 and cannot be used for the external RADIUS server.

Radius Port — Specify the port on which the RADIUS accounting server is listening.

Shared Secret — Specify a shared secret for accounting authentication for the hotspot. The shared secret is required to match the shared secret on the external RADIUS accounting server.

Timeout — Set the timeout value in seconds (1-255) used to timeout users accessing the RADIUS Accounting server if they have not successfully accessed the Accounting Server.

Retries — Define the number of retries (1-10) the user is allowed to access the RADIUS Accounting Server if the first attempt fails. The default is 1.

8 Refer to the *Radius Configuration* field to define a primary and secondary RADIUS server port and shared secret password.

Select mode — Use the *Select mode* drop-down menu to define whether an Internal or External server is to be used for the primary server.

Pri Server IP — Define the IP address of the primary RADIUS server. This is the address of your first choice for RADIUS server.

Pri Port — Enter the TCP/IP port number for the server acting as the primary RADIUS server. The default port is 1812.

Pri Secret — Enter the shared secret password used with the primary RADIUS Server.

Sec Server IP — Define the IP address of the secondary RADIUS server. This is the address of your second choice for RADIUS server.

Sec Port — Enter the TCP/IP port number for the server acting as the secondary RADIUS server. The default port is 1812.

Sec Secret — Enter the shared secret password used with the secondary RADIUS Server.

9 Click *OK* to save any changes to the Hotspot Configuration screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

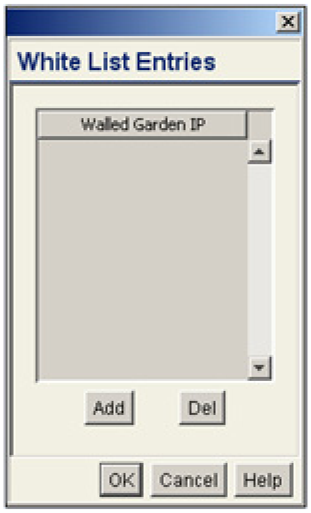
10 Click *Cancel* (if necessary) to undo any changes made. Cancel reverts the settings displayed on the Hotspot Configuration screen to the last saved configuration.

Defining the Hotspot White List

To host a Login, Welcome or Fail page on the external Web server, the IP address of that Web server should be in Access Point's White List.

NOTE

If using an external Web Server over the WAN port, and the hotspot's HTTP pages (login or welcome) redirect to the Access Point's WAN IP address for CGI scripts, the IP address of the external Web server and the Access Point's WAN IP address should be entered in the White List.



When a client requests a URL from a Web server, the login handler returns an HTTP redirection status code (for example, 301 Moved Permanently), which indicates to the browser it should look for the page at another URL. This other URL can be a local or remote login page (based on the hotspot configuration). The login page URL is specified in the location's HTTP header.

To host a Login page on the external Web server, the IP address of the Web server should be in the White list (list of IP addresses allowed to access the server) configuration. Ensure the Login page is designed so the submit action always posts the login data on the Access Point.

To define the White List for a target WLAN:

1. Click the *White List Entries* button from within the WLAN's Hotspot Config screen.
2. Click the *Add* button to define an IP address for an allowed destination IP address.
3. Select a White List entry and click the *Del* button to remove the address from the White List.
4. Click *OK* to return to the Hotspot Config screen where the configuration can be saved by clicking the Apply button.

   Now user enters his/her credentials on Login page and submits the page. Login Handler will execute a CGI script, which will use this data as input.
5. Click *Cancel* to return to the Hotspot Config screen without saving any of the White List entries defined within the White List Entries screen.

Customizing a Hotspot Display

Each access point WLAN can have a unique hotspot configured and mapped to that WLAN. This enables each Access Point WLAN to have an optimized hotspot configuration and applet display in respect to the WLAN's client support needs.

The hotspot's login, welcome and fail (login failure) pages are separate HTML files that can be content customized for each WLAN using a *cascading style sheet* (css). These screens can be customized in one of two ways:

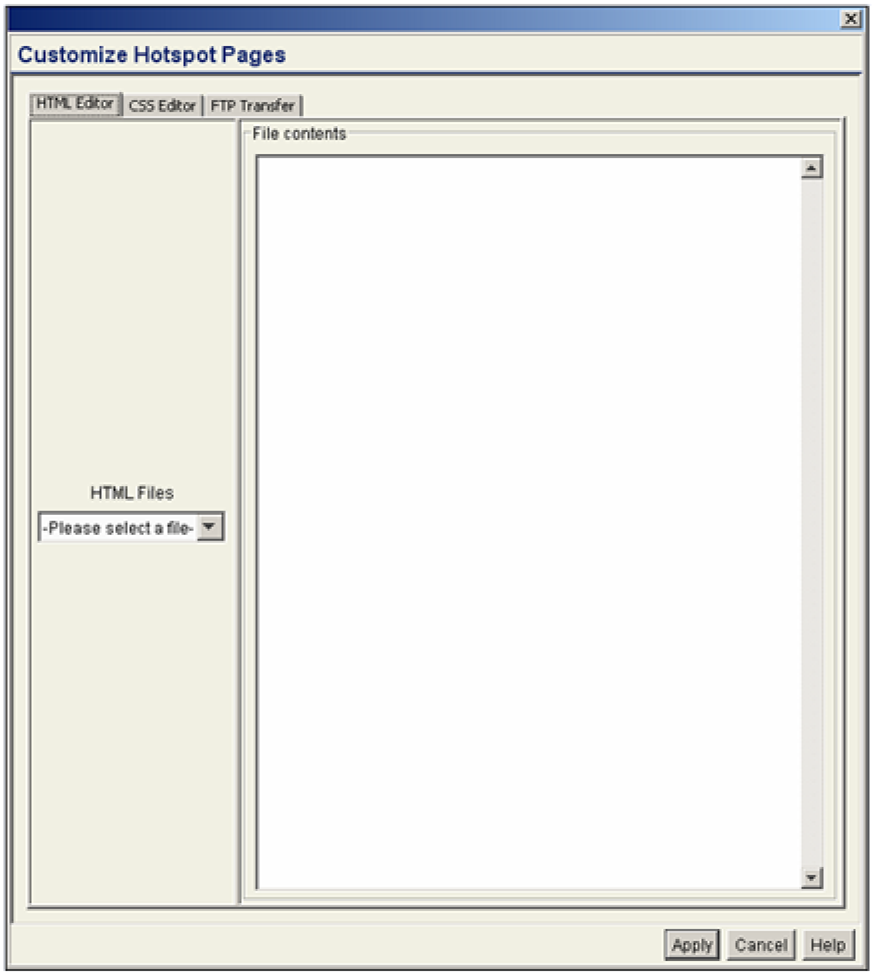
- By customizing the text and fonts displaying within the screens
- By customizing the properties (background color, logos etc.) of the screens themselves

The css contains the styling information for all the elements on the screens. This includes the font of displayed text as well as image placement and sizing. The css contains an exhaustive list of text and image properties which can altered by professional installer to customize the appearance of the hotspot.

Extreme Networks provides a default set of HTML files for the login, welcome and fail pages, and one css file that's referenced by these HTML files. The professional installer is also provided two default images which can be manipulated as required. Thus by default, each hotspot directory contains 3 HTML files, 1 css file and 2 images (small and large logos). Of these 5 files, the css file is used to customize the other pages. The files are hosted on the Access Point and imported to clients via an FTP download option provided by the Access Point's applet and the CLI. Once the css and HTML file editing is completed, they can be exported back to the access using FTP again.

To configure a customized WLAN hotspot:

1. Ensure the *Enable Hotspot* checkbox is selected from within the target WLAN screen, and ensure the WLAN is properly configured.
2. Click the *Configure Hotspot* button within the WLAN screen to display the *Hotspot Configuration* screen for that target WLAN.
3. Select *Customize Hotspot Pages* from within the *Internal Web Page Configuration* field.
4. Define the customized text you would like displayed for this WLAN's login, welcome and failure pages by selecting each page from the *HTML Files* drop-down menu.



The HTML Editor enables you to customize the hotspot html code. It displays the login.html, welcome.html and fail.html files (depending on user selection) in an editable text area.

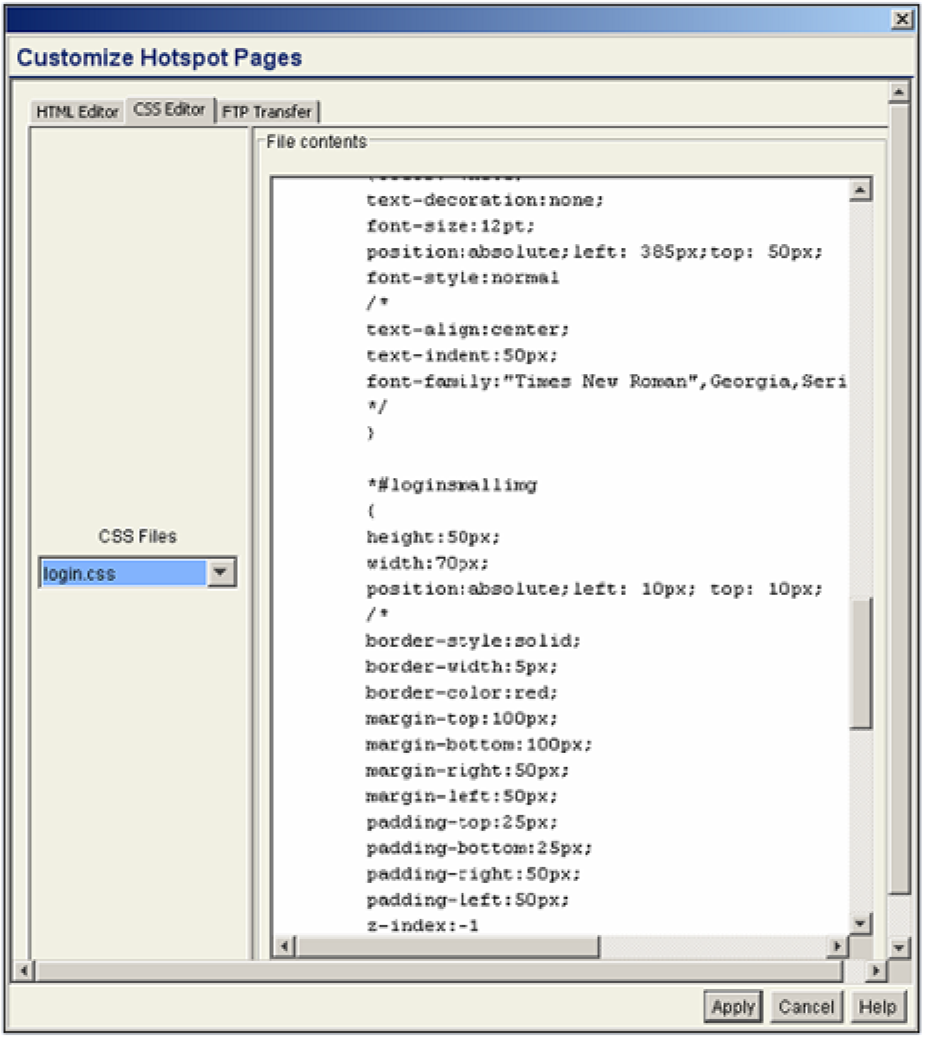
CAUTION

No file in a hotspot directory can exceed 10 kb. The maximum number of characters that can be entered into the text area is 10240.

5 Select *Apply* to save the updates made thus far.

6 Select the *CSS Editor* tab to review a guide describing css file customizations impacting how screens display for this WLAN's hotspot.

The CSS Editor tab contains descriptions of each field that can be manipulated within the css file. It also contains parameter options that can be used to change the appearance of the HTML screens. Thus, the CSS Editor tab is like a help file available as customizations are made to the css file.



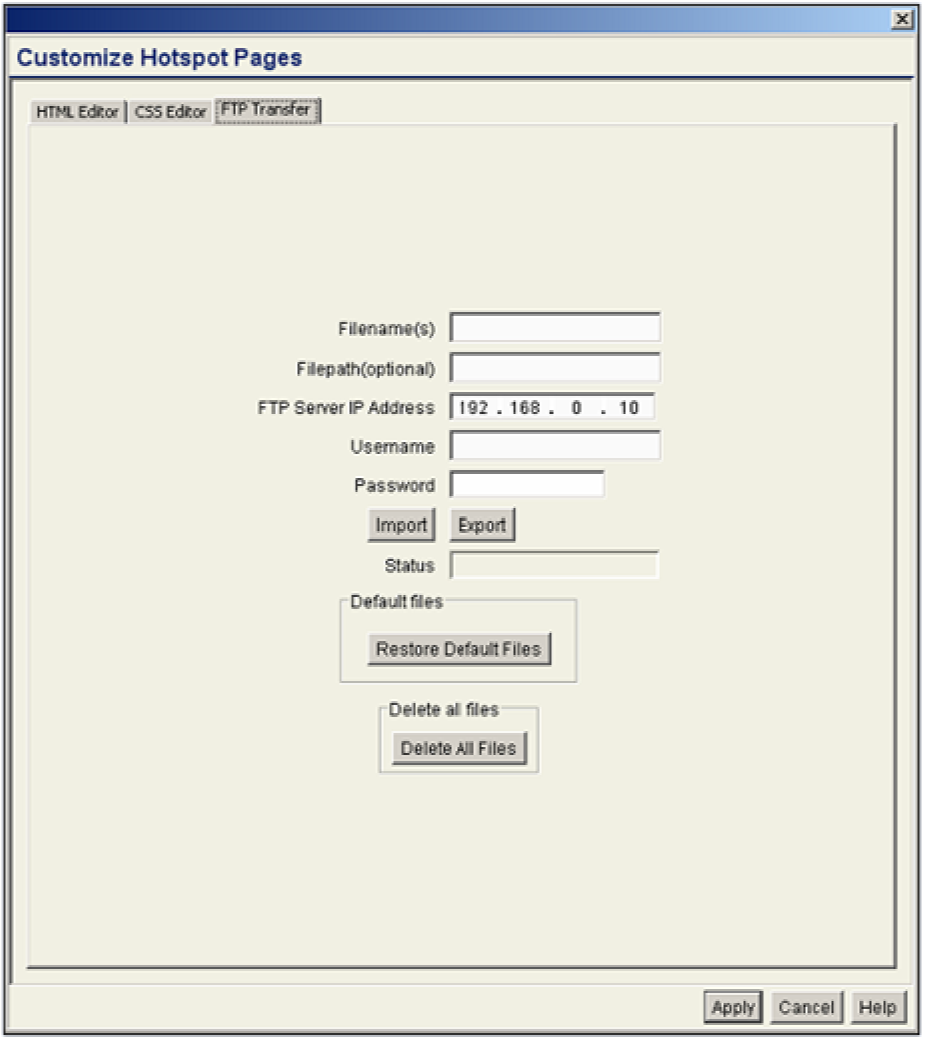
```
        text-decoration:none;
        font-size:12pt;
        position:absolute;left: 385px;top: 50px;
        font-style:normal
        /*
        text-align:center;
        text-indent:50px;
        font-family:"Times New Roman",Georgia,Seri
        */
        }

        *#loginsmallimg
        {
        height:50px;
        width:70px;
        position:absolute;left: 10px; top: 10px;
        /*
        border-style:solid;
        border-width:5px;
        border-color:red;
        margin-top:100px;
        margin-bottom:100px;
        margin-right:50px;
        margin-left:50px;
        padding-top:25px;
        padding-bottom:25px;
        padding-right:50px;
        padding-left:50px;
        z-index:-1
```

CAUTION

Once updated, the CSS file must not exceed 12500 bytes, or it cannot be exported back onto the Access Point for effective deployment with the hotspot.

7 Select the *FTP Transfer* tab to define the configuration of the FTP server configuration and target filename used to import or export the CSS and logo banners to and from the hosting Access Point.



FTP Server IP Address 192 . 168 . 0 . 10

Filename(s)
Provide the name of the target file either imported or exported from the FTP server. Up to 10 files can be used, and each must not exceed 39 characters.

Filepath(optional)
Optionally provide the path to the hotspot files specified within the Filenames field. The path cannot exceed 39 characters.

FTP Server IP Address
Enter the IP address of the FTP server used by the Access Point to import and export hotspot file information to the clients providing hotspot access.

Username
Specify a username to be used when logging in to the FTP server.

Password
Define a password allowing access to the FTP server for the hotspot import or export operation.

Import
Select the *Import* button to begin an FPT transfer from the hosting Access Point to the hotspot enabled client. Refer to the Status field for the results of the import operation. Selecting Import also saves the configuration before performing the import operation.

Export — Select the *Export* button to begin an FPT transfer from the hotspot enabled client to the hosting Access Point. Refer to the Status field for the results of the export operation. Selecting Export also saves the configuration before performing the export operation.

Status — Displays the Pass or Fail designation of the most recent import or export operation.

8 Select the *Restore Default Files* button to overwrite the customized files created on behalf of this WLAN and replace them with the default files provided with the Access Point firmware.

CAUTION

Extreme Networks recommends exporting any file present required for further development on to an external FTP server since they will all be lost during the restore operation.

9 Select the *Delete All Files* button to clear (delete) the hotspot directory for that particular WLAN so the user can better utilize the space in that hotspot's directory.

10 Click *Apply* to save the changes made within the FTP Transfer tab.

Setting the WLAN's Radio Configuration

Each access point WLAN can have a separate 802.11a/n or 802.11b/g/n radio configured and mapped to that WLAN. This enables each WLAN to optimize its radio configuration in respect to its intended client needs.

The Access Point displays one of three different radio configuration pages depending on which model SKU is purchased. The *Radio Configuration* screen enables you to configure one radio for 802.11a/n use and the other for 802.11b/g/n (no other alternatives exist for the dual-radio model).

The Altitude 4750 model Access Point is available in a three-radio model. The third Altitude 4750 radio is never a WLAN radio. The third radio is either disabled or set to WIPS mode depending on the radio configuration option selected from the Quick Setup screen. With the three-radio Altitude 4750 model, a third tab (Radio 3) has been added to the Radio Configuration screen. All of the other WLAN configurable elements available in either of the Radio 1 and Radio 2 tabs have been removed from the Radio 3 tab as they do not apply to WIPS support.

NOTE

The WIPS Server designation and radio configuration is set as part of the Access Point's quick setup. For more information on the quick setup configuration and how to define WIPS radio support, see "Configuring Device Settings" on page 67. For a description of WIPS functionality and how it relates to Access Point operation, see "Sensor Support" on page 23.

Altitude 4710	**Description**
Dual Radio	Two radios supporting either WLAN or WIPS (mutually exclusive)

Altitude 4750	Description
Three Radios	Two radios supporting either WLAN or WIPS. Radio three dedicated to WIPS.

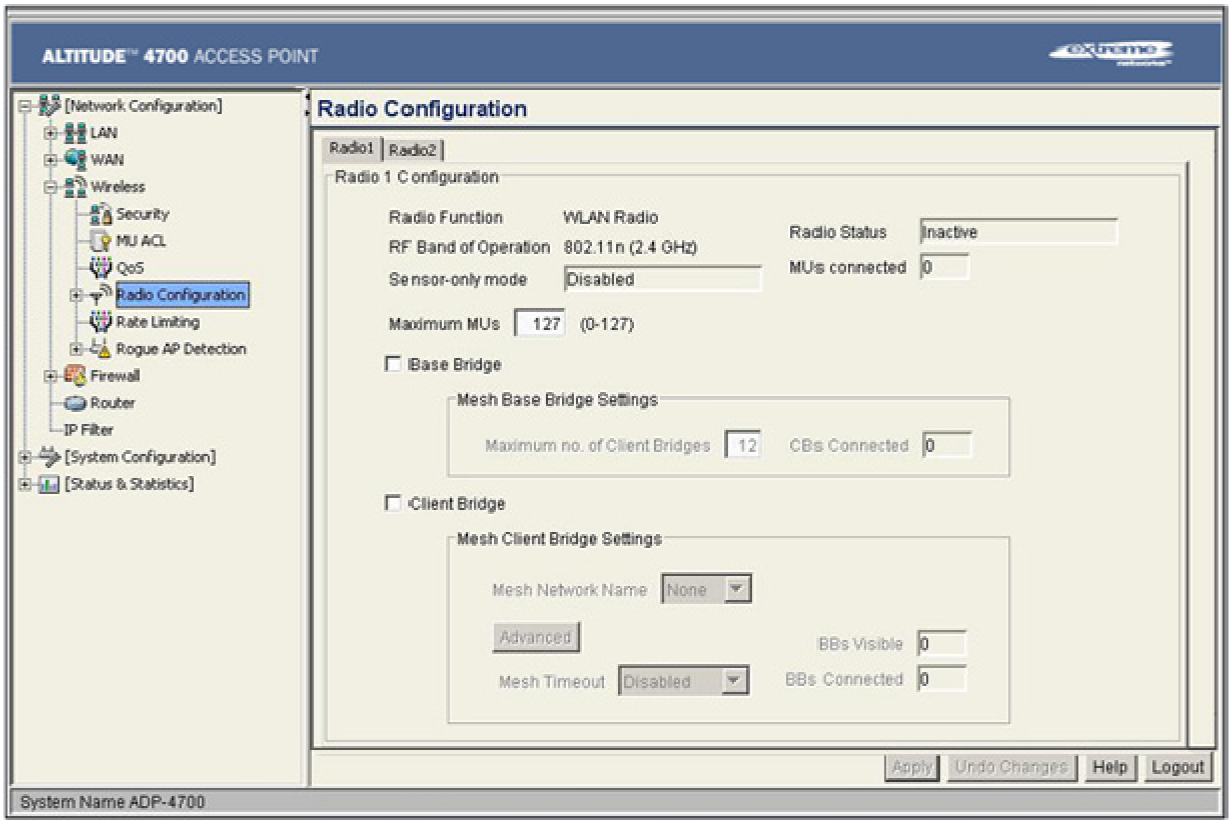
For radios 1 and 2, WIPS and WLAN modes are mutually exclusive. In WLAN mode, a radio functions as a traditional Access Point, providing wireless bridging. In WIPS mode a radio provides no wireless bridging. Instead, the radio performs the following functionality:

- *Wireless Termination*—The Access Point attempts to force an unwanted (or unauthorized) connection to disconnect.
- *Wireless Sniffing*—All received frames are reported to the WIPS server. This feature provides the WIPS server with visibility into the activity on the wireless network. The WIPS server processes the received traffic and provides the IT administrator with useful information about the 802.11 RF activities in the enterprise.
- *Spectrum Analysis*—The data needed to provide the current RF Spectrum is provided to the WIPS server. The Access Point does not display the data, but it is available to the WIPS server. Spectrum analysis can operate only when there are no WLAN radios configured. The WIPS daemon and server are responsible for limiting operation only when there is no radio in WLAN mode. When a configuration change is made at the AP, the Spectrum Analysis operation stops.
- *Live View*—The WIPS application provides a live view of the sensors, APs and MUs operating in a WLAN. Live view support exists throughout the WIPS application, wherever a device icon appears in an information panel or navigation tree. Access Live View by right-clicking on the device, which automatically limits the data to the specific device your choose.

The Radio Configuration screen displays with tabs. One tab for each Access Point radio. Verify tabs are selected and configured separately to enable the radio(s), and optionally set their mesh network definitions.

To set the access point radio configuration (this example is for a dual-radio Access Point):

1 Select *Network Configuration > Wireless > Radio Configuration* from the access point menu tree.



Radio Configuration

Radio 1 Configuration

Radio Function: WLAN Radio
RF Band of Operation: 802.11n (2.4 GHz)
Sensor-only mode: Disabled
Radio Status: Inactive
MUs connected: 0
Maximum MUs: 127 (0-127)

□ Base Bridge

Mesh Base Bridge Settings
Maximum no. of Client Bridges: 12
CBs Connected: 0

□ Client Bridge

Mesh Client Bridge Settings
Mesh Network Name: None
Advanced
BBs Visible: 0
Mesh Timeout: Disabled
BBs Connected: 0

System Name ADP-4700

Review the *Radio Function* to assess if this radio is currently functioning as a WLAN radio or has been dedicated as a sensor.

Refer to *RF Band of Operation* parameter to ensure you are enabling the correct 802.11a/n or 802.11b/g/n radio. After the settings are applied within this Radio Configuration screen, the *Radio Status* and *MUs connected* values update. If this is an existing radio within a mesh network, these values update in real-time.

NOTE

This section describes mesh networking (setting the radio's base and client bridge configuration) at a high level. For a detailed overview on the theory of mesh networking, see "Mesh Networking Overview" on page 577. For detailed information on the implications of setting the mesh configuration, see "Configuring Mesh Networking Support" on page 581. To review mesh network deployment scenarios, see "Mesh Network Deployment - Quick Setup" on page 590.

Refer to the *Sensor-only mode* parameter to discern whether this Access Point radio has been set to function as WLAN radio (normal operation) or as a dedicated sensor (no WLAN support available). The Access Point is set as a sensor radio using either the Access Point's *Quick Setup* screen or using a CLI command. Sensor mode support is disabled by default. For more information on using the Quick Setup screen to define the radio mode, see "Basic Device Configuration" on page 65.

2 Set the *Maximum MUs* between 0–127.

The maximum number of MUs that can associate to a single AP is 127. Therefore, the possible number of MUs that can associate to each radio is between 0 and 127.

NOTE

With a multiple-radio AP, a radio can be configured as either a Rogue AP or WIPS detector, not for just WLAN MU support.

NOTE

The AP does not support MU radio associations if its Maximum MUs value is set to 0. Alternatively, if you set the value to 127 for one radio, you risk shutting out MU associations for the other radio(s), as the AP does not validate the logic of a user's MU association distribution.

3 Select the *Base Bridge* checkbox to allow the radio to accept client bridge connections from other Access Points in client bridge mode. The base bridge is the acceptor of mesh network data from those client bridges within the mesh network and never the initiator.

4 If the Base Bridge checkbox has been selected, use the *Max# Client Bridges* parameter to define the client bridge load on a particular base bridge.

The maximum number of client bridge connections per radio is 12, with 24 representing the maximum for dual-radio models.

CAUTION

An Access Point in Base Bridge mode logs out whenever a Client Bridge associates to the Base Bridge over the LAN connection. This problem is not experienced over the Access Point's WAN connection. If this situation is experienced, log-in to the Access Point again.

Once the settings within the Radio Configuration screen are applied (for an initial deployment), the current number of client bridge connections for this specific radio displays within the *CBs Connected* field. If this is an existing radio within a mesh network, this value updates in real-time.

CAUTION

A problem could arise if a Base Bridge's Indoor channel is not available on an Outdoor Client Bridge's list of available channels. As long as an Outdoor Client Bridge has the Indoor Base Bridge channel in its available list of channels, it can associate to the Base Bridge.

5 Select the *Client Bridge* checkbox to enable the Access Point radio to initiate client bridge connections with other mesh network supported Access Point's using the same WLAN.

If the Client Bridge checkbox has been selected, use the *Mesh Network Name* drop-down menu to select the WLAN (ESS) the client bridge uses to establish a wireless link. The default setting, is (WLAN1). Extreme Networks recommends creating (and naming) a WLAN specifically for mesh networking support to differentiate the Mesh supported WLAN from non-Mesh supported WLANs.

CAUTION

The WLAN supporting hotspot clients must exist on the Base Bridge as well as Client Bridge. An MU is successfully authenticated by the Base Bridge only if the WLAN exists on both the Base Bridge and the Client Bridge. Additionally, the user group has to be associated with a WLAN on the Base Bridge for hotspot authentication to work.

CAUTION

An Access Point in client bridge mode cannot use a WLAN configured with a Kerberos or EAP 802.1x based security scheme, as these authentication types secure user credentials not the mesh network itself.

NOTE

Ensure you have verified the radio configuration for both Radio 1 and Radio 2 before saving the existing settings and exiting the Radio Configuration screen.

Once the settings within the Radio Configuration screen are applied (for an initial deployment), the current number of base bridges visible to the radio displays within the *BBs Visible* field, and the number of base bridges currently connected to the radio displays within the *BBs Connected* field. If this is an existing radio within a mesh network, these values update in real-time.

6 Click the *Advanced* button to define a prioritized list of Access Points to define Mesh Connection links. For a detailed overview on mesh networking and how to configure the radio for mesh networking support, see “Configuring Mesh Networking Support” on page 581.

7 If using a dual-radio model Access Point, refer to the *Mesh Timeout* drop-down menu to define whether one of the radio’s beacons on an existing WLAN or if a client bridge radio uses an uplink connection. The following drop-down menu options are available:

Disabled
When disabled, both radios are up at boot time and beaconing. If one radio (radio 1) does not have a mesh connection, the other radio (radio 2) is not affected. Radio 2 continues to beacon and associate MUs, but MUs can only communicate amongst themselves using the Access Point. Disabled is the default value.

Uplink Detect
When Uplink Detect is selected, the Access Point only boots up the radio configured as a client bridge. The Access Point boots up the second radio as soon as the first mesh connection is established. However, if the client bridge radio loses its uplink connection, the second radio shuts down immediately. Uplink detect is the recommended setting within a multi-hop mesh network.

Enabled
If the mesh connection is down on one radio (radio 1), the other radio (radio 2) is brought down and stops beaconing after the timeout period (45–65535 seconds). This allows the client bridge (radio 1) to roam without dropping the MUs associated to radio 2. The disadvantage is that radio 2 may beacon for the timeout period and have to drop associated MUs because radio 1 could not establish its uplink. The default timeout period is 45 seconds.

NOTE

The Mesh Time Out variable overrides the Ethernet Port Time Out (EPTO) setting on the LAN page when the Access Point is in bridge mode. As long as the mesh is down, the Access Point acts in accordance to the Mesh Time Out setting regardless of the state of the Ethernet. However, if the Ethernet goes down and the mesh link is still up, the EPTO takes effect.

For a detailed overview on mesh networking and how to configure the radio for mesh networking support, see “Configuring Mesh Networking Support” on page 581.

8 Click *Apply* to save any changes to the Radio Configuration screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

CAUTION

When defining a Mesh configuration and changes are saved, the mesh network temporarily goes down. The Mesh network is unavailable because the Access Point radio is reconfigured when applying changes. This can be problematic for users making changes within a deployed mesh network. If updating the mesh network using a LAN connection, the Access Point applet loses connection and the connection must be re-instated. If updating the mesh network using a WAN connection, the Access Point applet does not lose connection, but the mesh network is unavailable until the changes have been applied.

9 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Radio Configuration screen to the last saved configuration.

10 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Once the target radio has been enabled from the *Radio Configuration* screen, configure the radio's properties by selecting it from the access point menu tree.

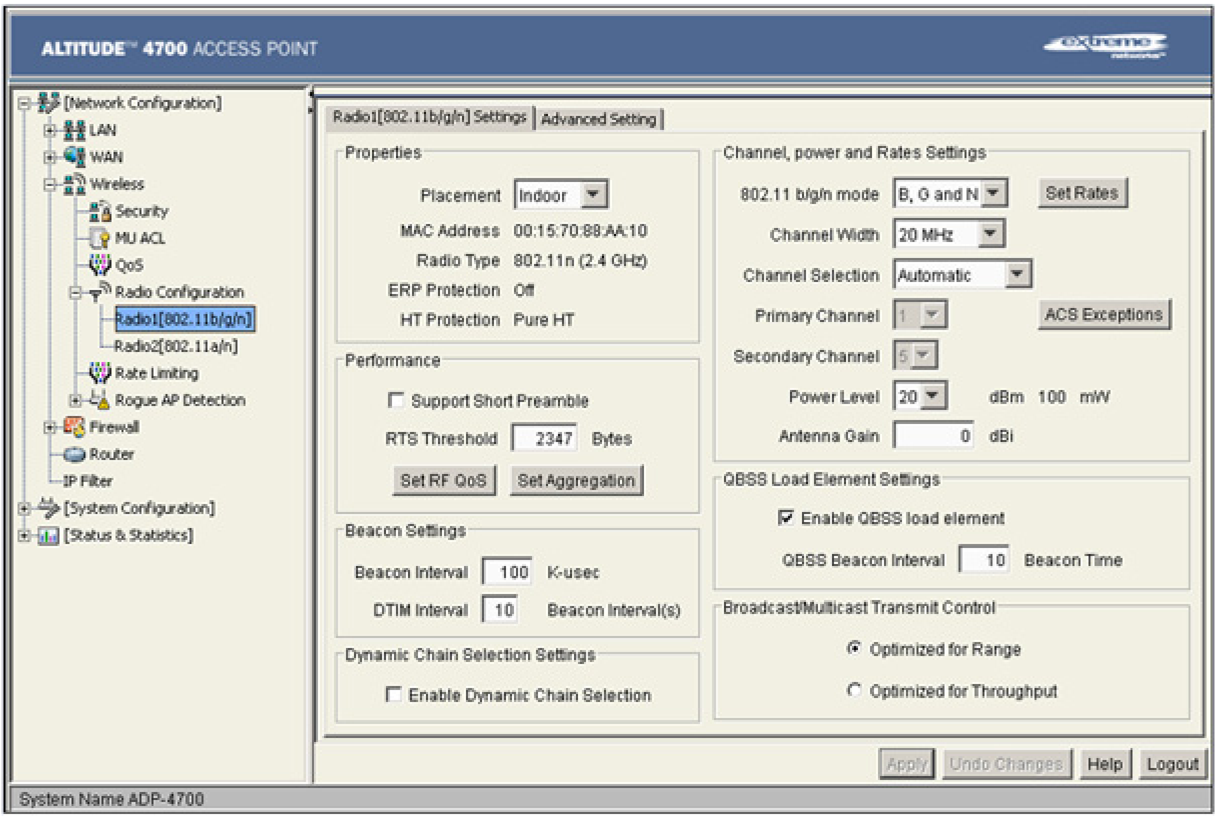
For more information, see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174.

Configuring the 802.11a/n or 802.11b/g/n Radio

Configure an 802.11a/n or 802.11b/g/n radio by selecting the radio's name (as defined using the 802.11a/n or 802.11b/g/n radio configuration screen described below) as a sub-menu item under the Radio Configuration menu item. Use the radio configuration screen to set the radio's placement properties, define the radio's threshold and QoS settings, set the radio's channel and antenna settings, define beacon and DTIM intervals and set the broadcast/multicast transmit control.

To configure the access point’s 802.11a/n or 802.11b/g/n radio:

1 Select *Network Configuration* > *Wireless* > *Radio Configuration* > *Radio1* (default name) from the access point menu tree.



Properties

Placement: Indoor

MAC Address: 00:15:70:88:AA:10

Radio Type: 802.11n (2.4 GHz)

ERP Protection: Off

HT Protection: Pure HT

Performance

□ Support Short Preamble

RTS Threshold: 2347 Bytes

Beacon Settings

Beacon Interval: 100 K-usec

DTIM Interval: 10 Beacon Interval(s)

Dynamic Chain Selection Settings

□ Enable Dynamic Chain Selection

Channel, power and Rates Settings

802.11 b/g/n mode: B, G and N

Channel Width: 20 MHz

Channel Selection: Automatic

Primary Channel: 1

Secondary Channel: 5

Power Level: 20 dBm 100 mW

Antenna Gain: 0 dBi

QBSS Load Element Settings

☑ Enable QBSS load element

QBSS Beacon Interval: 10 Beacon Time

Broadcast/Multicast Transmit Control

● Optimized for Range

○ Optimized for Throughput

System Name ADP-4700

2 Configure the *Properties* field to assign a name and placement designation for the radio.

Placement — Use the *Placement* drop-down menu to specify whether the radio is located outdoors or indoors. Default placement depends on the country of operation selected for the access point.

MAC Address — The access point, like other Ethernet devices, has a unique, hardware encoded *Media Access Control (MAC)* or IEEE address. MAC addresses determine the device sending or receiving data. A MAC address is a 48-bit number written as six hexadecimal bytes separated by colons. For example: *00:A0:F8:24:9A:C8.*

Radio Type — The *Radio Type* parameter simply displays the radio type as 802.11a/n or 802.11b/g/n. This field is read only and always displays the radio type selected from the access point menu tree under the Radio Configuration item.

ERP Protection — *Extended Rate PHY* (ERP) allows 802.11g MUs to interoperate with 802.11b only MUs. ERP Protection is managed automatically by the Access Point and informs users when 802.11b MUs are present within the Access Point’s coverage area. The presence of 802.11b MUs within the 802.11g coverage area negatively impacts network performance, so this feature should looked to as an indicator of why network performance has been degraded.

HT Protection

Displays the HT Protection state, and whether a non HT protected MU is currently associated with the Access Point.

3 Configure the *Channel, Power and Rate Settings* field to assign a channel, antenna diversity setting, radio transmit power level and data rate.

CAUTION

When deploying a mesh network, Extreme Networks recommends manually configuring channels and not using the Automatic or Uniform options.

802.11 b/g/n mode

For radio1, specify *B, G and N*, *B and G*, *G Only*, *B only* or *N Only* to define whether the 802.11b/g/n radio transmits in the 2.4 GHz band exclusively for 802.11b (legacy) clients or transmits in the 2.4 GHz band for 802.11g/n clients. Selecting b and g enables the access point to transmit to both b and g clients if legacy clients (802.11b) partially comprise the network. Select accordingly based on the MU requirements of the network.

The rates for the Access Point’s 2.4 GHz radio are as follows:

B, G and N—Allows only basic rates (default setting).

B and G—Allows 11b basic rates. Does not allow MCS rates.

G and N—Requires basic rates (either 6, 12, 24 or 1, 2, 5.5, 11, 6, 12, 24).

G Only—Requires one 11g basic rate. Does not allow MCS rates.

B Only—Allows for 11b rates only. Does not allow G or N rates.

N Only—Requires basic MCS rates.

Note: If the mode is B and G, the Channel Width option is not available, and a Secondary Channel cannot be defined.

For the 5 GHz radio, specify *A and N*, *A Only* or *N Only* to define whether the 802.11a/n radio transmits in the 5 Ghz band exclusively for 802.11a clients, 802.11n clients or transmits in the 5 Ghz band for both 802.11a/n clients.

A Only—Allows 11a rates.

N Only—Requires basic MCS rates.

A and N—Allows only 11a basic rates (default setting).

Channel Width

Select the Channel Width (MHz) from the drop-down menu. The AP radio can support 20 and 40 MHz channel widths. 20 MHz is the default setting for the 2.4 GHz radio. 20/40 MHz operation (the default setting for the 5 GHz radio) allows the Access Point to receive packets from clients using 20 MHz of bandwidth while transmitting a packet using 40 MHz bandwidth. This mode is supported for 11n users on both the 2.4 and 5 GHz radios. If an 11n user selects two channels (a Primary and Secondary channel), the system is configured for dynamic 20/40 operation.

When 20/40 is selected, clients can take advantage of "wider channels." 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Define a value as needed depending on the channel used. This field is not available when B and G is selected as the 802.11 b/g/n mode.

Channel Selection

The following channel selection options exist:

User Selected—This is the default setting. If 20/40 MHz is selected as the Channel Width (supporting 11n), the *Secondary Channel* drop-down menu becomes enabled. The user must define the primary channel first. Then, depending on the primary channel defined, the secondary channel list is filled with channels making the combination of primary and secondary channels valid. The actual channels available depend on regulatory domain requirements.

Automatic—When the Access Point is booted, the Access Point scans non-overlapping channels listening for beacons from other Access Points. After the channels are scanned, it will select the channel with the fewest Access Points. In the case of multiple Access Points on the same channel, it will select the channel with the lowest average power level.

The *Random* option is available for use with the 802.11a/n radio. To comply with *Dynamic Frequency Selection* (DFS) requirements in the European Union, the 802.11a/n radio uses a randomly selected channel each time the Access Point is powered on.

Power Level

Use the drop-down menu to defines the transmit power of the 802.11a/n or 802.11b/g/n antenna(s). The values are expressed in dBm and mW.

Antenna Gain	Set the antenna gain used with the selected antenna type between 0.00–15.00 dBm. The Access Point’s *Power Management Antenna Configuration File* (PMACF) automatically configures the Access Point’s radio transmit power based on the antenna type (provided in the CLI), its antenna gain (provided here) and the deployed country’s regulatory domain restrictions. Once the antenna type and gain are provided, the Access Point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Extreme Networks recommends that only a professional installer set the antenna gain and the antenna type.

Set Rates

Click the *Set Rates* button to define minimum and maximum data transmit rates for the radio.

Use the *Basic Rates* drop-down menu to select the rates available for either the 2.4 GHz or 5 GHz radio band. The menu options differ, based on the radio band.
For 2.4 GHz, the following options are available:

- 1 and 2 Mbps
- 1, 2, 5.5 and 11 Mbps (default setting)
- 1, 2, 5.5, 11 and 6, 12, 24 Mbps
- 1, 2, 5.5, 11 and 6, 12, 24 Mbps and MCS 0-7
- 6, 12 and 24 Mbps
- 6, 12 and 24 Mbps and MCS 0-7
- MCS 0-7

For 5 Ghz, the following options are available:

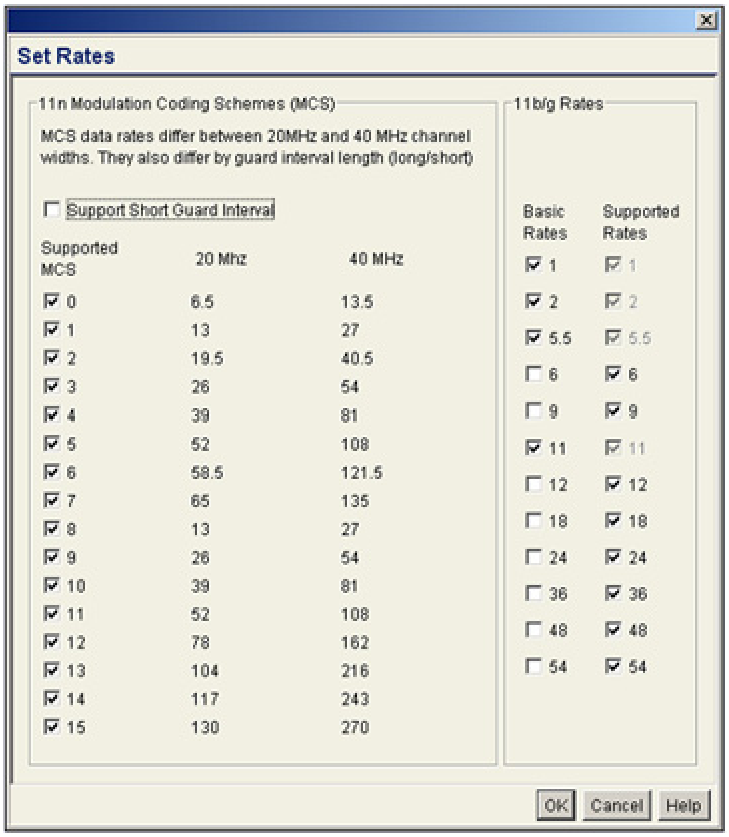
- 6, 12 and 24 Mbps
- 6, 12 and 24 Mbps and MCS 0-7
- MCS 0-7

When a basic rate option is selected (from the drop-down menu), the rates are automatically selected and grayed out in the *Supported Rates* radio boxes. Select remaining rates as needed for additional supported rates.

Enable the *Support Short Guard Interval* checkbox to set a guard interval (for interference protection) for 20 MHz and 40 MHz channel widths. When enabled, the AP's radio defines values to enable a packet to be transmitted with guard interval based on the configuration and capabilities of associated clients. Clients can associate to an Access Point regardless of whether they support a short guard interval.

If supporting 802.11n, select a *Supported MCS* index (0-15). Set a MCS *(modulation and coding scheme)* in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. MUs can associate as long as they support basic MCS (as well as non-11n basic rates).

Click *OK* to implement the selected rates and return to the radio configuration screen. Clicking *Cancel* reverts the Set Rates screen to the last saved configuration.



Set Rates

11n Modulation Coding Schemes (MCS)

MCS data rates differ between 20MHz and 40 MHz channel widths. They also differ by guard interval length (long/short)

☐ Support Short Guard Interval

Supported MCS	20 Mhz	40 MHz
☑ 0	6.5	13.5
☑ 1	13	27
☑ 2	19.5	40.5
☑ 3	26	54
☑ 4	39	81
☑ 5	52	108
☑ 6	58.5	121.5
☑ 7	65	135
☑ 8	13	27
☑ 9	26	54
☑ 10	39	81
☑ 11	52	108
☑ 12	78	162
☑ 13	104	216
☑ 14	117	243
☑ 15	130	270

11b/g Rates

Basic Rates	Supported Rates
☑ 1	☑ 1
☑ 2	☑ 2
☑ 5.5	☑ 5.5
☐ 6	☑ 6
☐ 9	☑ 9
☑ 11	☑ 11
☐ 12	☑ 12
☐ 18	☑ 18
☐ 24	☑ 24
☐ 36	☑ 36
☐ 48	☑ 48
☐ 54	☑ 54

4 Configure the *Performance* field to set the preamble, thresholds values and QoS values for the radio.

Support Short Preamble Interval	The preamble is approximately 8 bytes of packet header generated by the Access Point and attached to a packet prior to transmission from the 802.11b radio. The preamble length for 802.11b transmissions is rate dependant. A short preamble is 50% shorter than a long preamble. Leave the checkbox unselected if in a mixed MU/AP environment, as MUs and the Access Point are required to have the same RF Preamble settings for interoperability. The default is Disabled. The preamble length for 802.11a and 802.11g transmissions is the same, with no long or short preamble lengths.
RTS Threshold	RTS allows the access point to use RTS (Request To Send) on frames longer than the specified length. The default is 2341bytes.

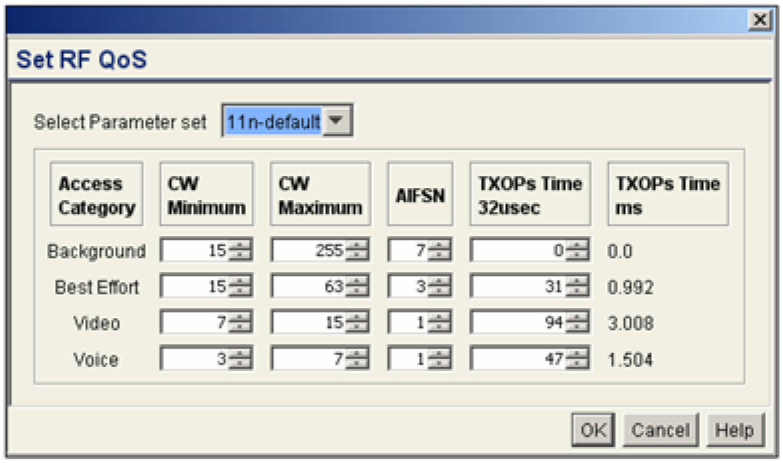
Set RF QoS

Click the *Set RF QoS* button to display the *Set RF QOS* screen to set QoS parameters for the radio. Do not confuse with the QoS configuration screen used for a WLAN. The Set RF QoS screen initially appears with default values displayed.

Select *manual* from the *Select Parameter set* drop-down menu to edit the *CW min* and *CW max* (contention window), *AIFSN (Arbitrary Inter-Frame Space Number)* and *TXOPs Time* for each Access Category. These are the QoS policies for the 802.11a/n or 802.11b/g/n radio, not the QoS policies configured for the WLAN (as created or edited from the *Quality of Service Configuration* screen).

Extreme Networks recommends only advanced users manually set these values. If the type of data-traffic is known, use the drop-down menu to select an option representative of the intended radio band support. Wifi represents multimedia traffic, default is typical data traffic and voice is for “Voice-Over-IP” supported wireless devices.

Click *OK* to implement the selected QoS values and return to the 802.11a/n or 802.11b/g/n radio configuration screen. Clicking *Cancel* reverts the screen to the last saved configuration.



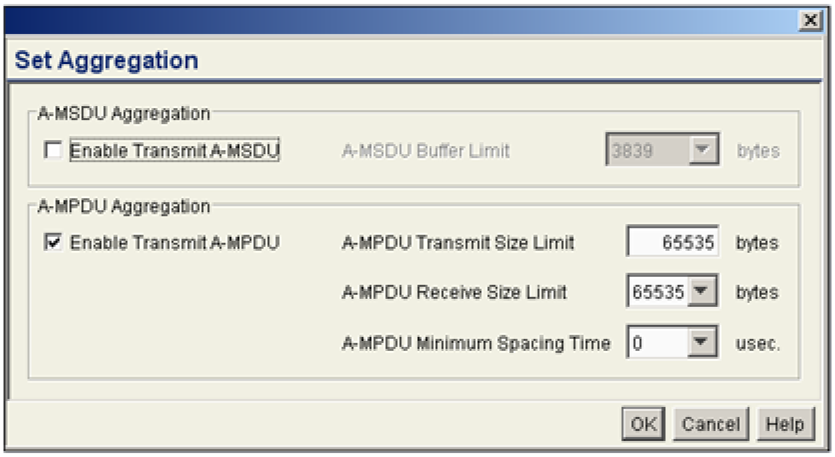
Select Parameter set 11n-default

Access Category	CW Minimum	CW Maximum	AIFSN	TXOPs Time 32usec	TXOPs Time ms
Background	15	255	7	0	0.0
Best Effort	15	63	3	31	0.992
Video	7	15	1	94	3.008
Voice	3	7	1	47	1.504

Set Aggregation

Select the *Enable Transmit A-MSDU* checkbox (within the A-MSDU Aggregation field) to enable the aggregation of MAC Service frames. When enabled, long frames can be both sent and received (up to 4 KB). The A-MSDU buffer limit is not user configurable. If disabled, no AMSDU packets are transmitted by the Access Point.

Select the *Enable Transmit A-MPDU* checkbox (within the A-MPDU Aggregation field) to allow the aggregation of MAC Protocol frames. When enabled, long frames can be both sent and received (up to 64 KB). When enabled, define an A-MPDU Transmit Size Limit (default is 2 bytes), A-MPDU Receive Size Limit (default is 65535 bytes) and an A-MPDU Minimum Spacing Time (default is 0 usec). Set these values as appropriate to broadcast the maximum length A-MPDU transmit and receive intervals that can be used.



Set Aggregation

A-MSDU Aggregation

☐ Enable Transmit A-MSDU — A-MSDU Buffer Limit: 3839 bytes

A-MPDU Aggregation

☑ Enable Transmit A-MPDU — A-MPDU Transmit Size Limit: 65535 bytes

A-MPDU Receive Size Limit: 65535 bytes

A-MPDU Minimum Spacing Time: 0 usec.

5 Refer to the *Beacon Settings* field to set the radio beacon and DTIM intervals.

Beacon Interval

The beacon interval controls the performance of power save stations. A small interval may make power save stations more responsive, but it will also cause them to consume more battery power. A large interval makes power save stations less responsive, but could increase power savings. The default is 100. Avoid changing this parameter as it can adversely affect performance.

DTIM Interval

The DTIM interval defines how often broadcast frames are delivered for each of the four Access Point BSSIDs. If a system has an abundance of broadcast traffic and it needs to be delivered quickly, Extreme Networks recommends decreasing the DTIM interval for that specific BSSID. However, decreasing the DTIM interval decreases the battery life on power save stations. The default is 10 for each BSSID. Extreme Networks recommends using the default value unless qualified to understand the performance risks of changing it.

6 Refer to the *Dynamic Chain Selection Settings* field to enable or disable Dynamic Chain Selection.

When enabled, dynamic chain selection forces an Access Point radio to transmit packets using legacy transmit rates (11b, 11g and/or 11a rates) using a single transmit chain. Transmissions utilizing 11n rates (MCS0–MCS15) continue to use a normal number of transmit chains, which may be 1, 2, or 3 depending on the configuration and power source. If dynamic chain selection is disabled, all transmissions utilize the same number of transmit chains. This feature is disabled by default.

7 Refer to the *QBSS Load Element Settings* field to determine whether channel usage data is transmitted to associated devices.

Enable QBSS load element

When enabled, the Access Point communicates channel usage data to associated devices using an interval you define. The QBSS load represents the percentage of time the channel is in use by the Access Point and the Access Point's MU count. This information is helpful in assessing the Access Point's overall load on a channel, its availability for additional device associations and multi media traffic support. This setting is enabled by default.

QBSS Beacon Interval

Set the QBSS beacon (transmission) interval the Access Point uses for sending QBSS data to associated devices.

8 Refer to the *Broadcast/Multicast Transmit Control* field to define the broadcast/multicast transmission configuration.

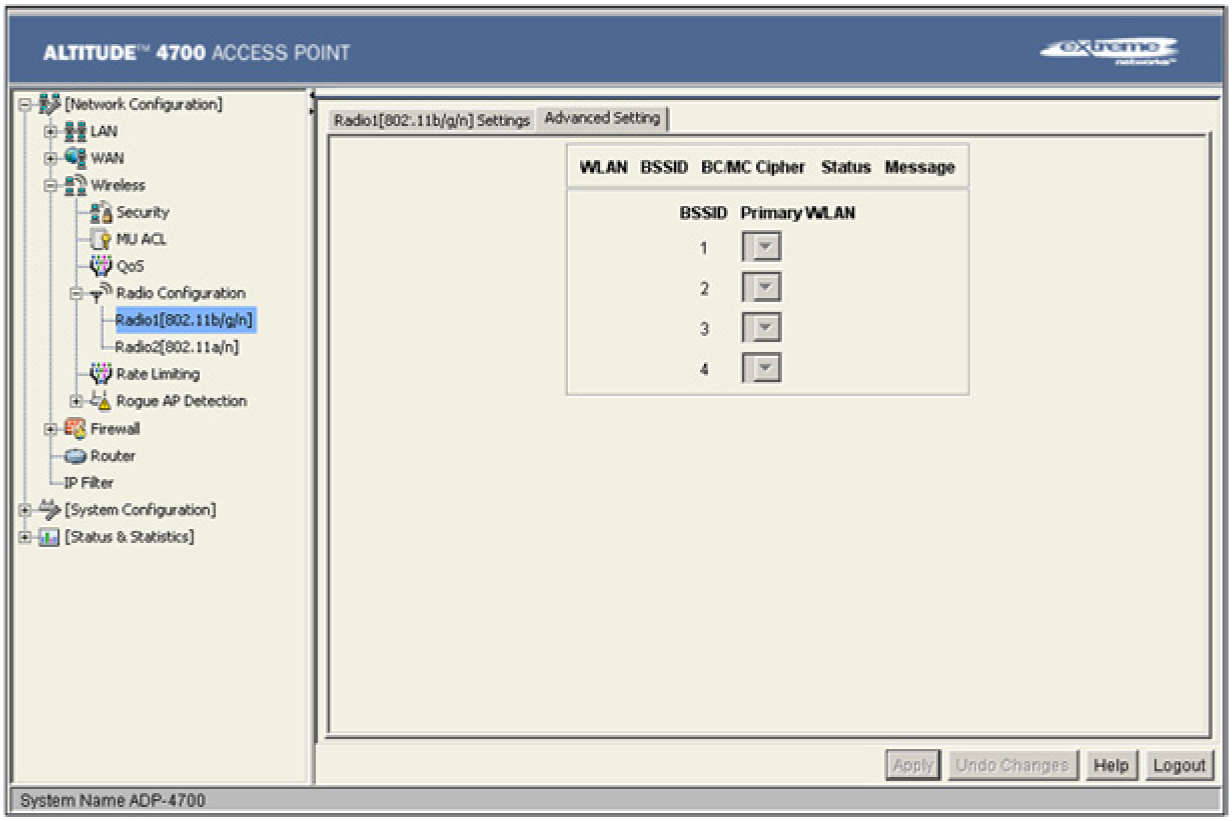
The *Optimized for Range* radio button is selected by default. This default option is ideal when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates selected from this radio's Set Rates screen.

Select the *Optimized for Throughput* radio button to transmit group packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where transmission range is secondary to broadcast/multicast transmission performance.

NOTE

Broadcast/multicast rate control is supported in both standalone and adaptive AP configurations and can be imported/exported as part of the Access Point's existing configuration import and export capability.

9 Select the *Advanced Settings* tab to strategically map BSSIDs to WLANs in order to define them as primary WLANs.



Defining Primary WLANs allows an administrator to dedicate BSSIDs (4 BSSIDs are available for mapping) to WLANs. From that initial BSSID assignment, Primary WLANs can be defined from within the WLANs assigned to BSSID groups 1 through 4. Each BSSID beacons only on the primary WLAN.

The user should assign each WLAN to its own BSSID. In cases where more than four WLANs are required, WLANs should be grouped according to their security policies so all of the WLANs on a BSSID have the same security policy. It is generally a bad idea to have WLANs with different security policies on the same BSSID, as this will result in warning or error messages.

NOTE

If using a dual-radio Access Point, 4 BSSIDs for the 802.11b/g/n radio and 4 BSSIDs for the 802.11a/n radio are available.

WLAN — Lists the WLAN names available to the 802.11a/n or 802.11b/g/n radio that can be assigned to a BSSID.

BSSID — Assign a BSSID value of 1 through 4 to a WLAN in order to map the WLAN to a specific BSSID.

BC/MC Cipher — A read only field displaying the downgraded BC/MC (Broadcast/Multicast) cipher for a WLAN based on the BSSID and VLAN ID to which it has been mapped.

Status — Displays the following color coded status:

Red—Error (Invalid Configuration)
Yellow—Warning (Broadcast Downgrade)
Green—Good (Configuration is OK)

Message — Displays the verbal status of the WLAN and BSSID assignments. If the Status column displays green, the Message will typically be *Configuration is OK*. If yellow, a description of invalid configuration displays.

10 Use the *Primary WLAN* drop-down menu to select a WLAN from those WLANs sharing the same BSSID. The selected WLAN is the primary WLAN for the specified BSSID.

11 Click *Apply* to save any changes to the Radio Settings and Advanced Settings screens. Navigating away from the screen without clicking Apply results in changes to the screens being lost.

12 Click *Undo Changes* (if necessary) to undo any changes made to the screen and its sub-screens. Undo Changes reverts the settings to the last saved configuration.

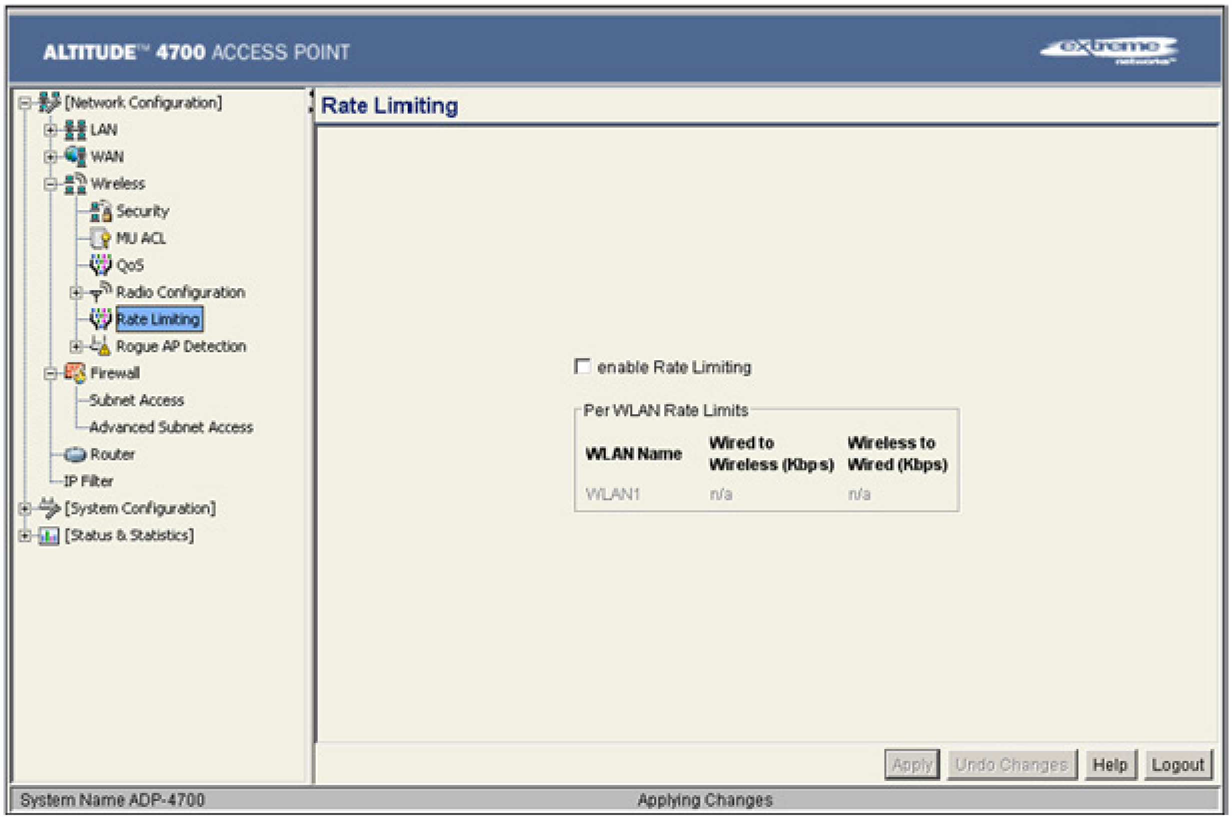
13 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring MU Rate Limiting

Use the *Rate Limiting* screen to control the MU rate limit allotted to individual WLANs. MU rate limiting enables an administrator to determine how much radio bandwidth is allowed to each MU within any one of the 16 supported AP WLANs. Rate limiting is on per a MU basis for the WLAN.

To define MU rate limits for specific WLANs on an Access Point radio:

1 Select *Network Configuration* > *Wireless* > *Rate Limiting* from the access point menu tree.



Rate Limiting

☐ enable Rate Limiting

Per WLAN Rate Limits

WLAN Name	Wired to Wireless (Kbps)	Wireless to Wired (Kbps)
WLAN1	n/a	n/a

System Name ADP-4700

Applying Changes

2 Select the *Enable Rate Limiting* option to globally enable MU rate limiting for each of the Access Point's 16 WLANs.

Once enabled, MU rate limiting still needs to be enabled for a specific WLAN, then the rate limit allocation needs to be defined for MU traffic within that specific WLAN. To modify a WLAN-to-radio assignment, see "Creating/Editing Individual WLANs" on page 148.

3 Refer to the *Per WLAN Rate Limits* field to review the rate limits defined thus far for any of the Access Point's 16 WLANs.

The rates are displayed in Kbps for both wired to wireless and wireless to wired traffic flows from the WLAN and its radio configuration.

4 Click *Apply* to save any changes to the Rate Limiting screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

5 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Rate Limiting screen to the last saved configuration.

6 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

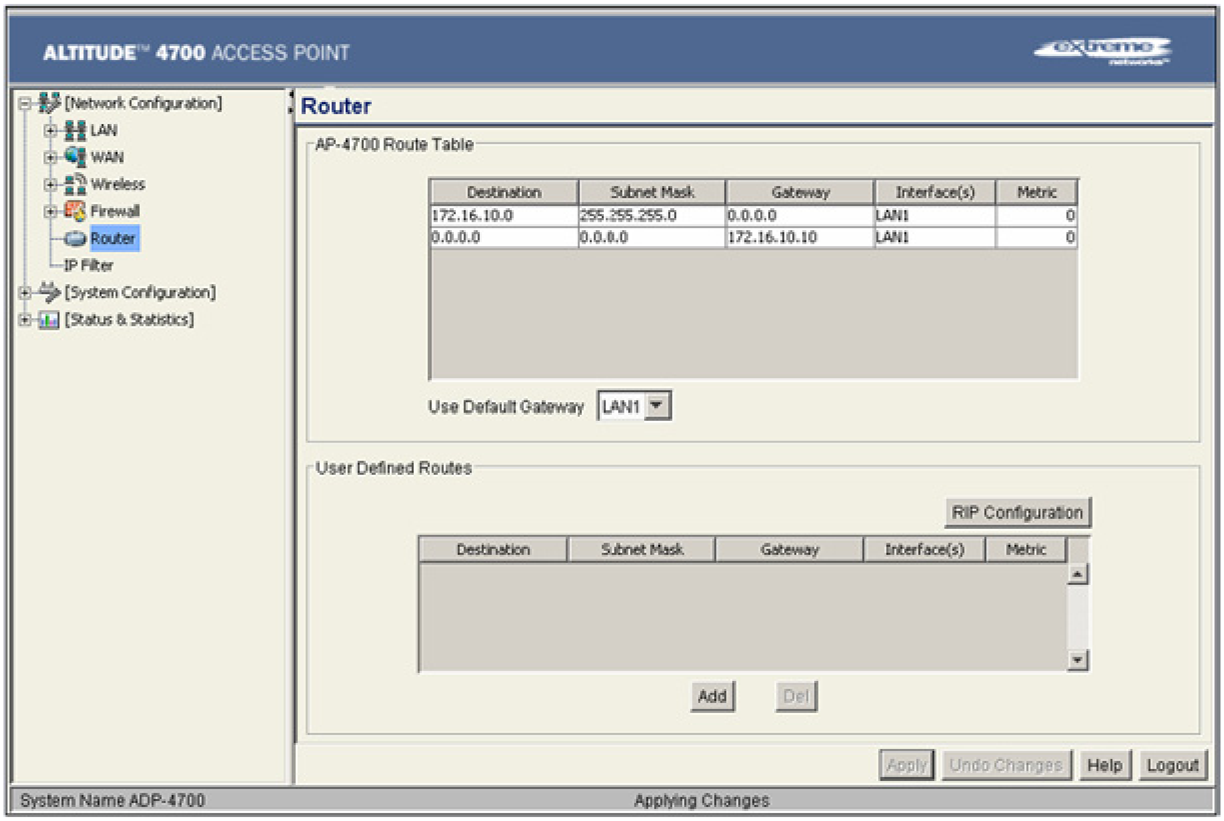
NOTE

Though the Rogue AP and Firewall features appear after the Rate Limiting features within the access point menu tree, they are described in "Configuring Access Point Security" on page 197, as both items are data protection functions. More specifically, see, “Configuring Firewall Settings” on page 218 and “Configuring Rogue AP Detection” on page 243.

Configuring Router Settings

The access point router uses routing tables and protocols to forward data packets from one network to another. The access point router manages traffic within the network, and directs traffic from the WAN to destinations on the access point managed LAN. Use the access point *Router* screen to view the router's connected routes. To access the Router screen.

1 Select *Network Configuration* > *Router* from the access point menu tree.



Router

AP-4700 Route Table

Destination	Subnet Mask	Gateway	Interface(s)	Metric
172.16.10.0	255.255.255.0	0.0.0.0	LAN1	0
0.0.0.0	0.0.0.0	172.16.10.10	LAN1	0

Use Default Gateway: LAN1

User Defined Routes

Destination	Subnet Mask	Gateway	Interface(s)	Metric

System Name ADP-4700 Applying Changes

2 Refer to the access point *Router Table* field to view existing routes.

The access point Router Table field displays a list of connected routes between an enabled subnet and the router. These routes can be changed by modifying the IP address and subnet masks of the enabled subnets.

The information in the access point Router Table is dynamically generated from settings applied on the *WAN* screen. The destination for each subnet is its IP address. The subnet mask (or network mask) and gateway settings are those belonging to each subnet. Displayed interfaces are those associated with destination IP addresses. To change any of the network address information within the WAN screen, see “Configuring WAN Settings” on page 135.

3 From the *Use Default Gateway* drop-down menu, select the WAN or either of the two LANs (if enabled) to server as the default gateway to forward data packets from one network to another.

4 To set or view the RIP configuration, click the *RIP Configuration* button.

Routing Information Protocol (RIP) is an interior gateway protocol that specifies how routers exchange routing-table information. The Router screen also allows the administrator to select the type of RIP and the type of RIP authentication used by the controller. For more information on configuring RIP, see "Setting the RIP Configuration" on page 187.

5 Use the *User Defined Routes* field to add or delete static routes.

The User Defined Routes field allows the administrator to view, add or delete internal static (dedicated) routes.

a Click the *Add* button to create a new table entry.

b Highlight an entry and click the *Del* (delete) button to remove an entry.

c Specify the destination IP address, subnet mask, and gateway information for the internal static route.

d Select an enabled subnet from the *Interface(s)* column's drop-down menu to complete the table entry. Information in the *Metric* column is a user-defined value (from 1 to 65535) used by router protocols to determine the best hop routes.

6 Click the *Apply* button to save the changes.

7 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

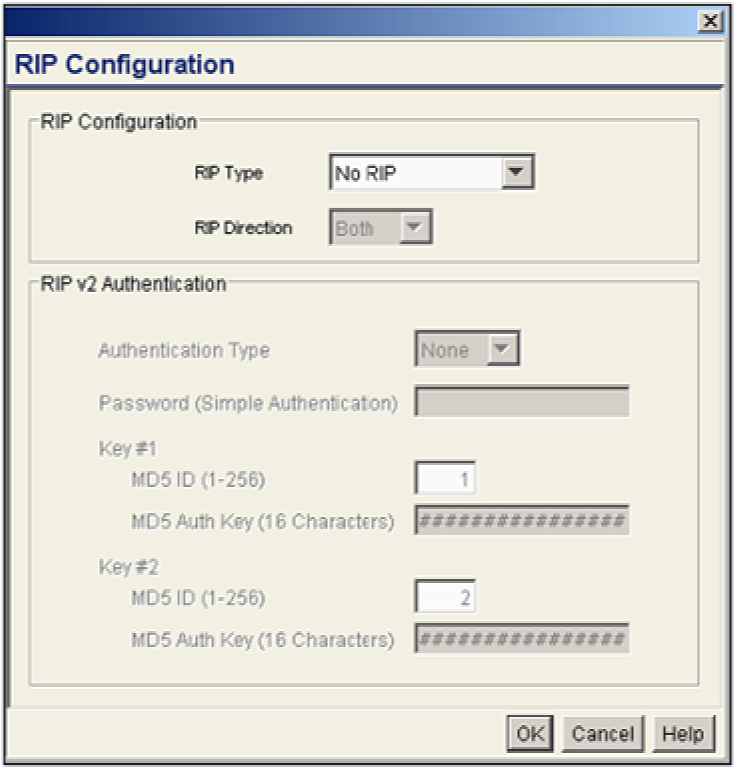
Setting the RIP Configuration

To set the RIP configuration:

1 From within the RIP Configuration field, select the RIP Type from the drop-down menu. The following options are available:

No RIP	The *No RIP* option prevents the Access Point's router from exchanging routing information with other routers. Routing information may not be appropriate to share, for example, if the Access Point manages a private LAN.
RIP v1	RIP version 1 is a mature, stable, and widely supported protocol. It is well suited for use in stub networks and in small autonomous systems that do not have enough redundant paths to warrant the overhead of a more sophisticated protocol.
RIP v2 (v1 compat)	RIP version 2 (compatible with version 1) is an extension of RIP v1's capabilities, but it is still compatible with RIP version 1. RIP version 2 increases the amount of packet information to provide the a simple authentication mechanism to secure table updates.
RIP v2	RIP version 2 enables the use of a simple authentication mechanism to secure table updates. More importantly, RIP version 2 supports subnet masks, a critical feature not available in RIP version 1. This selection is not compatible with RIP version 1 support.

2 Select a routing direction from the *RIP Direction* drop-down menu. *Both* (for both directions), *Rx only* (receive only), and *TX only* (transmit only) are available options.



RIP Configuration

RIP Type: No RIP

RIP Direction: Both

RIP v2 Authentication

Authentication Type: None

Password (Simple Authenticaton):

Key #1

MD5 ID (1-256): 1

MD5 Auth Key (16 Characters): ################

Key #2

MD5 ID (1-256): 2

MD5 Auth Key (16 Characters): ################

3 If RIP v2 or RIP v2 (v1 compat) is the selected RIP type, the *RIP v2 Authentication* field becomes active. Select the type of authentication to use from the *Authentication Type* drop-down menu. Available options include:

None — This option disables the RIP authentication.

Simple — This option enables RIP version 2's simple authentication mechanism. This setting activates the Password (Simple Authentication) field.

MD5 — This option enables the MD5 algorithm for data verification. MD5 takes as input a message of arbitrary length and produces a 128-bit fingerprint. The MD5 setting activates the RIP v2 Authentication settings for keys (below).

4 If the Simple authentication method is selected, specify a password of up to 15 alphanumeric characters in the *Password (Simple Authentication)* area.

5 If the MD5 authentication method is selected, fill in the *Key #1* field (Key #2 is optional). Enter any numeric value between 0 and 256 into the *MD5 ID* area. Enter a string consisting of up to 16 alphanumeric characters in the *MD5 Auth Key* area.

6 Click the *OK* button to return to the Router screen. From there, click *Apply* to save the changes.

Configuring IP Filtering

Use the Access Point's IP filtering functionality to determine which IP packets are processed normally by the Access Point and which are discarded. If discarded, a packet is deleted and ignored (as if never received). The allow/deny mechanism used by IP filtering makes it similar to an *access control list* (ACL).

IP filtering supports the creation of up to 20 filter rules enforced at layer 3. Once defined (using the Access Point's SNMP, GUI or CLI), filtering rules can be enforced on the Access Point's LAN1 or LAN2 interfaces and within any of the 16 Access Point WLANs. An additional default action is also available denying traffic when filter rules fail. Lastly, imported and exported configurations retain their defined IP filtering configurations.

IP filtering is a network layer facility. The IP filtering mechanism does not know anything about the application using the network connections, only the connections themselves. For example, you can deny user access to an internal network on the default telnet port, but if you rely on IP filtering alone, you cannot stop people from using the telnet program with a port you allow to pass through your firewall.

There are a couple of important rules a packet adheres to when its compared with the filter policy list:

- Packets are always filtered in sequential order (filtering always begins with the first filter policy displayed in the IP Filtering screen, then the second, third, and so on). The *IP Filtering* screen is invoked for LANs within the LAN1 or LAN2 screen and for WLANs within the New WLAN or Edit WLAN screen. It's from this screen that allow or deny designations are set for IP filtering.
- Packets are compared with lines of the filter policy list until a match is made. Once a packet matches a line of the list, it's acted upon, and no further comparisons take place. If inspected packets are determined to not be IP packets, it permitted by the Access Point for its inbound or outbound destination.

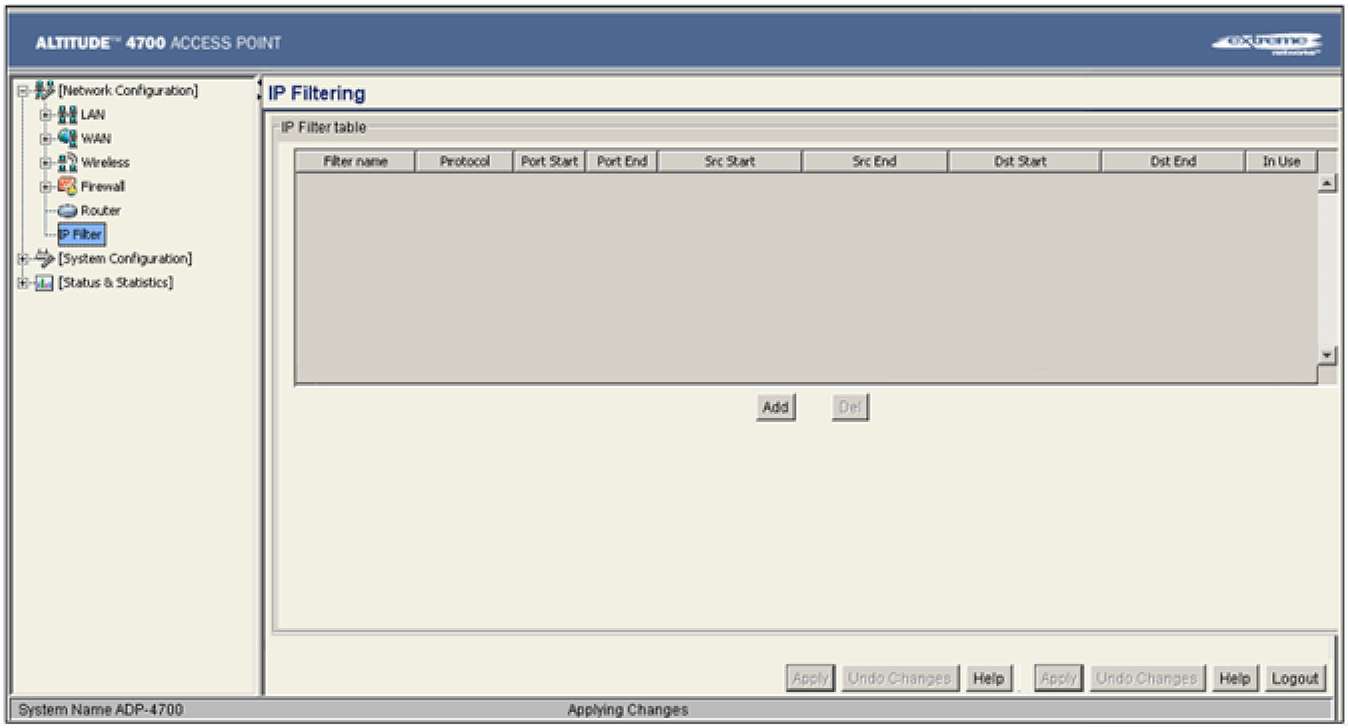
Once you create a filter policy, apply it to an interface in either an incoming or outgoing direction.

- Traffic entering the Access Point's LAN1, LAN2 or WLAN (1-16) from a client is classified as *Incoming* traffic.
- Traffic leaving the Access Point's LAN1, LAN2 or WLAN (1-16) in route to a client is classified as *Outgoing* traffic.

For additional examples of how to configure IP Filter policies for both an Access Point WLAN and LAN, see "IP Filter Configuration - Example" on page 192.

To filter packets against undesired data traffic:

1 Select *Network Configuration* > *IP Filtering* from the access point menu tree.



When the IP Filtering screen is initially displayed, there are no default filtering policies, and they must be created.

NOTE

With IP Filtering, users can only define a destination port, not a source port.

2 Click the *Add* button to define the attributes of a new IP Filtering policy. The following policy (or filtering rule) attributes require definition.

Filter name
: Create a name for the filter policy unique to its function in order to differentiate it from others that may have somewhat similar configurations.

Protocol
: Specify the protocol used for the filter policy. The options are *ALL*, *TCP, UDP, ICMP, PIM, GRE, RSVP, IDP, PUP, EGP, IPIP, ESP, AH, IGMP, IPVG, COMPR_H and RAW_IP.*

Port Start
: Defines the socket number (or port) number representing the beginning protocol port range either allowed or denied permission to the target LAN1, LAN2 or WLAN.

Port End
: Defines the socket number (or port) number representing the ending protocol port range either allowed or denied permission to the target LAN1, LAN2 or WLAN.

Src Start — Creates a range beginning source IP address to be either allowed or denied IP packet forwarding. The source address is where the packet originated. Setting the Src End value the same as the Src Start allows or denies just this address without defining a range.

Src End — Providing this address completes a range of source (data origination) addresses than can either be allowed or denied access to the LAN1, LAN2 or WLAN.

Dst Start — Creates a range beginning destination IP address to be either allowed or denied IP packet forwarding. Setting the Dst End value the same as the Dst Start allows or denies just this address without defining a range.

Dst End — Providing this address completes a range of destination addresses than can either be allowed or denied access to the LAN1, LAN2 or WLAN.

In Use — Displays YES if the listed filter policy is currently being utilized by LAN1, LAN2 or a WLAN. NO is displayed if the listed policy is currently not be utilized by either of the LAN ports or any of the Access Point's 16 WLANs.

NOTE

Once filter policies have been defined, they can then be applied to traffic on either of the two Access Point LAN ports or any of the 16 Access Point WLANs. The procedure for applying a filtering policy is the same, as both the LAN1/LAN2 and WLAN screens display the same IP Filtering sub screen for this operation. For more information, see "Applying a Filter to LAN1, LAN2 or a WLAN (1-16)" on page 191.

3. If necessary, select an existing policy and select the *Del* button to permanently remove the filtering policy from those available.
4. Click *Apply* to save any changes to the IP Filtering screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.
5. Click *Undo Changes* to securely exit the IP Filtering screen without saving your changes.
6. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Applying a Filter to LAN1, LAN2 or a WLAN (1-16)

Once filter policies are defined, they must be applied to a LAN or WLAN within the LAN1 or LAN2 screens, or within the WLAN's New/Edit screens, not from within the main IP Filtering menu.

To apply an existing IP filter policy to LAN1, LAN2 or a WLAN:

1. Display the IP Filtering menu.

   From the LAN1 or LAN2 screen:

   a. Select *Network Configuration > LAN > LAN1 (or LAN2)* from the access point menu tree.

   b. Select the *Enable IP Filtering* button in the lower, right-hand side of the screen.

   c. Select the *IP Filtering* button.

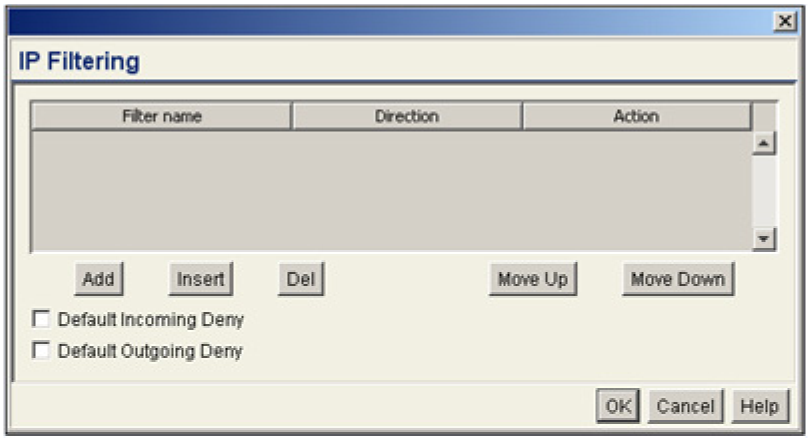
From the Wireless screen:

a Select *Network Configuration* > *Wireless* from the access point menu tree.

b Click the *Create* button to apply the filter to a new WLAN, or highlight an existing WLAN and click the *Edit* button. Either the *New WLAN* or *Edit WLAN* screen displays.

c Select the *Enable IP Filtering* button in the lower portion of the screen.

d Select the *IP Filtering* button.



The screen displays with both the *Default Incoming Deny* and *Default Outgoing Deny* checkboxes selected by default. Consequently, if you enable IP filtering but do not apply any filters that allow IP traffic, then no IP traffic will be forwarded, as the default deny settings have precedence.

2 Use the *Filter name* drop menu to select an existing filter.

3 Set the *Direction* as Incoming or Outgoing as required.

4 Apply an *Action* of Allow or Deny to permit or restrict the rules of this filter in the direction selected.

5 Select *Add* to apply the filter(s) (and their rules and permissions) to the LAN or WLAN.

6 Click *OK* add the IP filter to the LAN or WLAN. Navigating away from the screen without clicking OK results in all changes to the screens being lost.

7 Click *Cancel* to securely exit the IP Filtering screen without saving your changes.

For additional examples of how to configure IP Filter policies for both an Access Point WLAN and LAN, see "IP Filter Configuration - Example" on page 192.

IP Filter Configuration - Example

The following describes how to setup a global filter, apply it to a WLAN or LAN and review statistics to assess the filter's configuration.

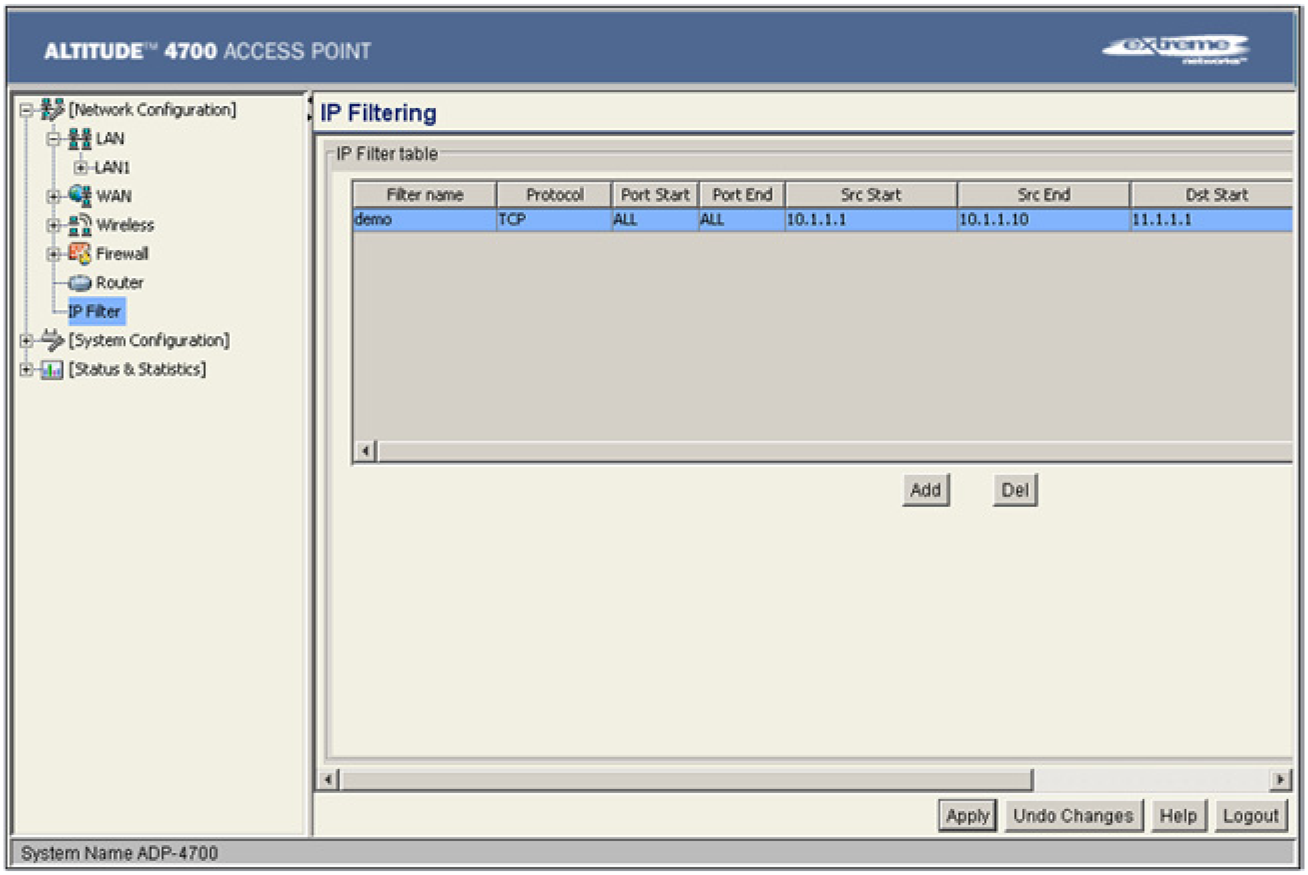
Creating a Global Filter

A global filter contains IP packet parameters that need to be matched where the filter is applied. These parameters include protocol number (TCP, ICMP etc.), port range, source IP range and destination IP range. Though an IP filter can be created using either the Access Point applet or CLI, the following example uses the CLI:

```
admin(network.ipfilter)>add icmp1 ICMP ALL ALL 10.1.1.1 10.1.1.10 11.1.1.1
11.1.1.10

admin(network.ipfilter)>show
--------------------------------------------------------------------------------
Idx Name         Protocol  Port-Start-End  SrcIP-Start-End  DstIP-Start-End  In-Use
--------------------------------------------------------------------------------
1    icmp1        ICMP      ALL             10.1.1.1         11.1.1.1          NO
                                            10.1.1.10        11.1.1.10
admin(network.ipfilter)>
```

Once created, the filter displays within the *Network Configuration > IP Filtering* screen.



IP Filtering

IP Filter table

Filter name	Protocol	Port Start	Port End	Src Start	Src End	Dst Start
demo	TCP	ALL	ALL	10.1.1.1	10.1.1.10	11.1.1.1

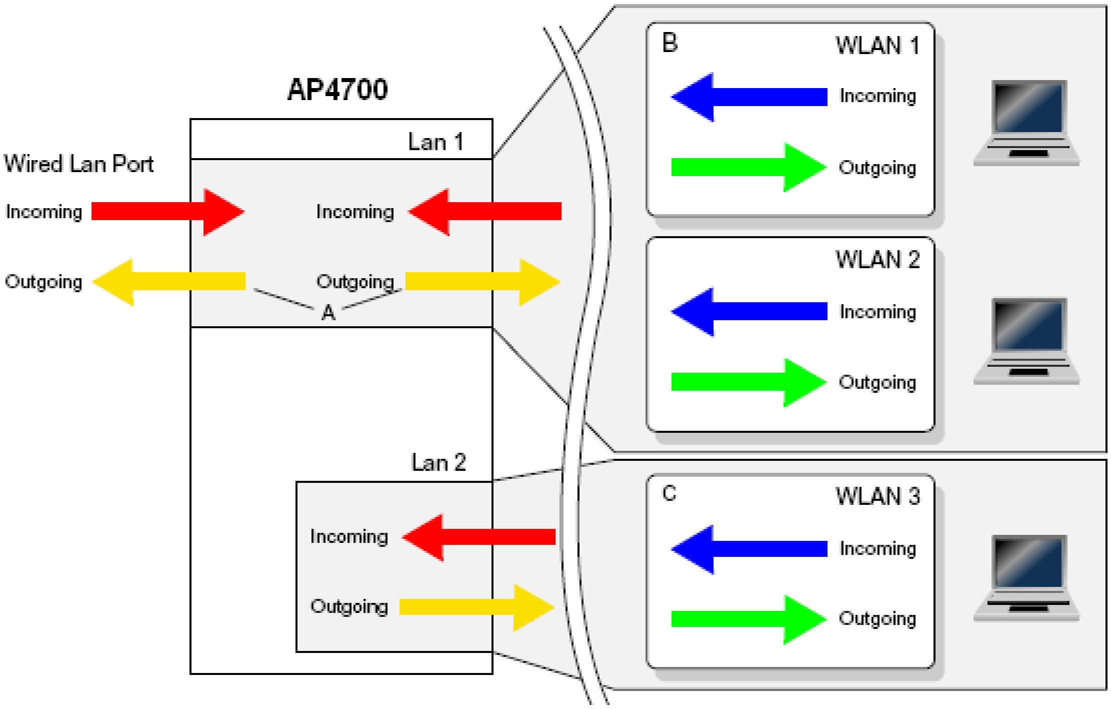
System Name ADP-4700

Applying the Filter to a WLAN or LAN

Once created, filters in the IP Filter Table can be applied to a WLAN or LAN. Refer to the following diagram to illustrate this point

NOTE

When both LAN IP filtering and WLAN IP filtering are enabled, a packet must pass the criteria of both LAN and WLAN filter policies.



Adding a filter to LAN 1 for outbound traffic results in the inspection of packets at point A. Both packets out the physical port and wireless transmissions are checked. Adding a filter to WLAN 1 for inbound traffic results in the inspection of packets at point B. Even though WLAN 2 is on LAN 1, its packets are unaffected. Adding a filter to WLAN 3 for inbound traffic results in the inspection of packets at point C.

Default rules must also be set upon enabling IP filtering on a LAN or WLAN. By default, when IP filtering is enabled, all inbound and outbound traffic is disabled. Default filters are applied when no other applied filter is matched.

When applying multiple filters, the filter which matches first is applied. In this sense the filter priority is the order of the list from top to bottom.

Creating a WLAN IP Filter Policy. The following example uses the Access Point CLI:

```
admin(network.wireless.wlan.ipfpolicy)>set mode 1 enable
admin(network.wireless.wlan.ipfpolicy)>add 1 icmp1 incoming deny
admin(network.wireless.wlan.ipfpolicy)>show 1

-------------------------------------------------------------------------
Idx Filter-Name             Direction      Action
-------------------------------------------------------------------------
1    icmp1                   incoming       deny

IP Filter Mode                      : enable
Default Incoming Action             : allow
Default Outgoing Action             : allow
admin(network.wireless.wlan.ipfpolicy)>
```

Creating a LAN IP Filter Policy. The following example uses the Access Point CLI:

```
admin(network.lan.ipfpolicy)>add 1 icmp1 incoming deny
admin(network.lan.ipfpolicy)>show 1
------------------------------------------------------------------
Idx Filter-Name          Direction      Action
------------------------------------------------------------------
1   icmp1                 incoming      deny

IP Filter Mode                    : enable
Default Incoming Action           : deny
Default Outgoing Action           : deny
admin(network.lan.ipfpolicy)>
```

NOTE

For information on applying a filter to a WLAN or LAN using the Access Point GUI applet, see, "Applying a Filter to LAN1, LAN2 or a WLAN (1-16)" on page 191.

Assessing IP Filter Stats

Detailed IP filter statistics can be displayed as follows from the Access Point CLI:

```
admin(stats)>show s-wlan 1

Name                           : joe
ESSID                          : joe
Authentication                 : No Authentication
Encryption                     : No Encryption
Radio/s                        : 802.11a, 802.11b/g
Number of Associated Clients   : 1

Traffic Information:

Packets per second:
Rx              : 0 pps
Tx                             : 0 pps
Total                          : 0 pps

<Hit any key to continue>
Throughput:
Rx                             : 0.00 Mbps
Tx                             : 0.00 Mbps
Total                          : 0.00 Mbps
Average Bit Speed              : 0.00 Mbps
%Non-Unicast Packets           : 0.00 %

RF Status:
Avg MU Signal                  : 0.0 dBm
Avg MU Noise                   : 0.0 dBm
Avg MU Signal-to-Noise         : 0.0 dB


Error Information:
Average Number of Retries      : 0.00 Retries
```

```
Dropped Packets                : 0.00 %
%Undecryptable Packets         : 0.00 %

IP Filtering:
Incoming:
icmp1                          : 0 denied
Default Action                 : 64 allowed
Outgoing:
Default Action                 : 75 allowed

admin(stats)>show lan 1

LAN Interface Information
LAN Interface 1                   : enable
IP Address 1                      : 192.168.0.1
Network Mask                      : 255.255.255.0
Ethernet Address                  : 0015700078C5
Speed                             : 100 Mbps
Duplex                            : full

LAN Rx Information
rx packets                        : 12520
rx bytes                          : 2663360
rx errors                         : 0
rx dropped                        : 0
Rx Overruns                       : 0
Rx Frame Errors                   : 0

LAN Tx Information
tx packets                        : 7105
tx bytes                          : 3236256
tx errors                         : 0
tx dropped                        : 0
Tx Overruns                       : 0
Tx Carrier Errors                 : 0

WLANs on this LAN :

IP Filtering:
Incoming:
icmp1                          : 0 denied
Default Action                 : 0 denied
Outgoing:
Default Action                 : 0 denied
```

6

CHAPTER

Configuring Access Point Security

Security measures for the access point and its WLANs are critical. Use the available access point security options to protect the access point LAN from wireless vulnerabilities, and safeguard the transmission of RF packets between the access point and its associated MUs.

WLAN security can be configured on an ESS by ESS basis on the access point. Sixteen separate ESSIDs (WLANs) can be supported on an access point, and must be managed (if necessary) between the 802.11a/n and 802.11b/g/n radio. The user has the capability of configuring separate security policies for each WLAN. Each security policy can be configured based on the authentication (Kerberos, 802.1x EAP) or encryption (WEP, KeyGuard, WPA/TKIP or WPA2/CCMP) scheme best suited to the coverage area that security policy supports.

The access point can also create VPN tunnels to securely route traffic through a IPSEC tunnel and block transmissions with devices interpreted as Rogue APs.

NOTE

Security for the access point can be configured in various locations throughout the access point menu structure. This chapter outlines the security options available to the access point, and the menu locations and steps required to configure specific security measures.

Configuring Security Options

To configure the data protection options available on the access point, refer to the following:

- To set an administrative password for secure access point logins, see “Setting Passwords” on page 198.
- To display security policy screens used to configure the authentication and encryption schemes available to the access point, see “Enabling Authentication and Encryption Schemes” on page 200. These security policies can be used on more than one WLAN.
- To create a security policy supporting 802.1x EAP, see “Configuring 802.1x EAP Authentication” on page 204.
- To define a security policy supporting Kerberos, see, “Configuring Kerberos Authentication” on page 202.
- To create a security policy supporting WEP, see “Configuring WEP Encryption” on page 208.

- To configure a security policy supporting KeyGuard, see, "Configuring KeyGuard Encryption" on page 209.
- To define a security policy supporting WPA-TKIP, see "Configuring WPA/WPA2 Using TKIP" on page 211.
- To create a security policy supporting WPA2-CCMP, see "Configuring WPA2-CCMP (802.11i)" on page 213.
- To create WLANs with same SSID but different BSSIDs and security schemes, see "Configuring Multi Cipher Support" on page 216.
- To configure the access point to block specific kinds of HTTP, SMTP and FTP data traffic, see "Configuring Firewall Settings" on page 218.
- To create VPN tunnels allowing traffic to route securely through a IPSEC tunnel to a private network, see "Configuring VPN Tunnels" on page 225.
- To configure the access point to block transmissions with devices detected as Rogue AP's (hostile devices), see "Configuring Rogue AP Detection" on page 243.

Setting Passwords

Before setting the access point security parameters, verify an administrative password for the access point has been created to restrict access to the device before advanced device security is configured.

To password protect and restrict access point device access:

1. Connect a wired computer to the access point LAN port using a standard CAT-5 cable.
2. Set up the computer for TCP/IP DHCP network addressing and make sure the DNS settings are not hardcoded.
3. Start Internet Explorer (with Sun Micro Systems' *Java Runtime Environment* (JRE) 1.5 or higher installed) and type in the default IP address in the address field.

   To connect to the Access Point, the IP address is required. If connected to the Access Point using the WAN port, the default static IP address is 10.1.1.1. The default password is "*admin123*." If connected to the Access Point using the LAN port, the default setting is DHCP client. The user is required to know the IP address to connect to the Access Point using a Web browser.

   The access point Login screen displays.

   NOTE

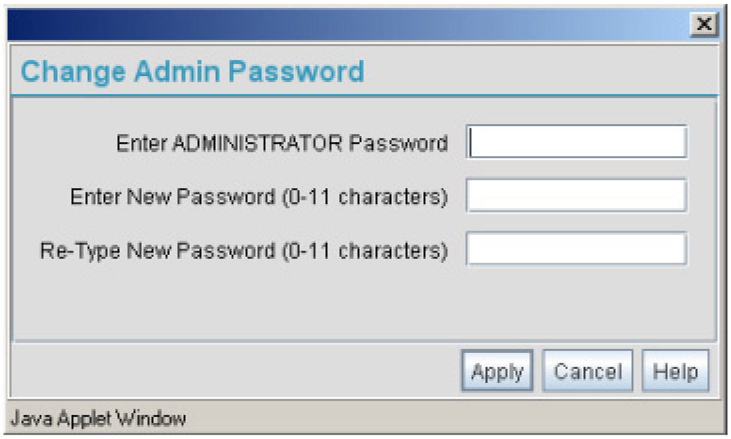
   For optimum compatibility use Sun Microsystems JRE 1.5 or higher (available from Sun's Web site), and be sure to disable Microsoft's Java Virtual Machine if it is installed.

   NOTE

   DNS names are not supported as a valid IP address for the access point. The user is required to enter a numerical IP address.

4. Log in using "*admin*" as the default Username and "*admin123*" as the default Password.

   If the default login is successful, the *Change Admin Password* window displays. Change the default login and password to significantly decrease the likelihood of hacking.



Change Admin Password

Enter ADMINISTRATOR Password

Enter New Password (0-11 characters)

Re-Type New Password (0-11 characters)

CAUTION

Restoring the Access Point's configuration back to default settings changes the administrative password back to "admin123." If restoring the configuration back to default settings, be sure you change the administrative password accordingly.

5 Enter the previous password and the new admin password in the two fields provided. Click the *Apply* button.

Once the admin password has been created/updated, the *System Settings* screen displays. If the access point has not had its System Settings (device name, location etc.) configured, see "Configuring System Settings" on page 78.

Once the password has been set, refer back to "Configuring Security Options" on page 197 to determine which access point security feature to configure next.

Resetting the Access Point Password

The Access Point has a means of restoring its password to its default value. Doing so also reverts the Access Point's security, radio and power management configuration to their default settings. Only an installation professional should reset the Access Point's password and promptly define a new restrictive password.

To contact Extreme Networks Support in the event of a password reset requirement, go to http://esupport.extremenetworks.com

CAUTION

Only a qualified installation professional should set or restore the Access Point's radio and power management configuration in the event of a password reset.

Enabling Authentication and Encryption Schemes

To complement the built-in firewall filters on the WAN side of the access point, the WLAN side of the access point supports authentication and encryption schemes. Authentication is a challenge-response procedure for validating user credentials such as username, password, and sometimes secret-key information. The access point provides two schemes for authenticating users: *802.1x EAP* and *Kerberos*.

Encryption applies a specific algorithm to alter its appearance and prevent unauthorized reading. Decryption applies the algorithm in reverse to restore the data to its original form. Sender and receiver must employ the same encryption/decryption method to interoperate.

Wired Equivalent Privacy (WEP) is available in two encryption modes: 40 bit (also called WEP 64) and 104 bit (also called WEP 128). The 104-bit encryption mode provides a longer algorithm (better security) that takes longer to decode (hack) than the 40-bit encryption mode.

Each WLAN (16 WLANs available in total to an access point regardless of the model) can have a separate security policy. However, more than one WLAN can use the same security policy. Therefore, to avoid confusion, do not name security policies the same name as WLANs. Once security policies have been created, they are selectable within the *Security* field of each *WLAN* screen. If the existing default security policy does not satisfy the data protection requirements of a specific WLAN, a new security policy (using the authentication and encryption schemes discussed above) can be created.

CAUTION

Mesh configurations do not support mismatched security policies when operating using a mixed mode scheme. Ensure the encryptions and authentication schemes used by APs in a mesh network are complimentary with one another.

To enable an existing WLAN security policy or create a new policy:

1 Select *Network Configuration* > *Wireless* > *Security* from the access point menu tree.

The *Security Configuration* screen displays.

2 If a new security policy is required, click the *Create* button.

The *New Security Policy* screen displays with the *Manually Pre-shared key/No authentication* and *No Encryption* options selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a guest network wherein no sensitive data is either transmitted or received.

However, selecting any other authentication or encryption checkbox displays a configuration field for the selected security scheme within the *New Security Policy* screen.

NOTE

An existing security policy can be edited from the Security Configuration screen by selecting an existing policy and clicking the Edit button. Use the Edit Security Policy screen to edit the policy. For more information on editing an existing security policy, refer to security configuration sections described in steps 4 and 5.

3 Use the *Name* field to define a logical security policy name.

Remember, multiple WLANs can share the same security policy, so be careful not to name security policies after specific WLANs or risk defining a WLAN to single policy. Extreme Networks recommends naming the policy after the attributes of the authentication or encryption type selected (for example, *WPA2 Allow TKIP*).

4 Enable and configure an *Authentication* option if necessary for the target security policy.

Manually Pre-Shared Key / No Authentication	Select this button to disable authentication. This is the default value for the *Authentication* field.
Kerberos	Select the *Kerberos* button to display the *Kerberos Configuration* field within the New Security Policy screen. For specific information on configuring Kerberos, see "Configuring Kerberos Authentication" on page 202.
802.1x EAP	Select the *802.1x EAP* button to display the *802.1x EAP Settings* field within the New Security Policy screen. For specific information on configuring EAP, see "Configuring 802.1x EAP Authentication" on page 204.

5 Enable and configure an *Encryption* option if necessary for the target security policy.

No Encryption	If *No Encryption* is selected, encryption is disabled for the security policy. If security is not an issue, this setting avoids the overhead an encryption protocol causes on the access point. No Encryption is the default value for the Encryption field.
WEP 64 (40-bit key)	Select the *WEP 64 (40 bit key)* button to display the *WEP 64 Settings* field within the New Security Policy screen. For specific information on configuring WEP 64, see "Configuring WEP Encryption" on page 208.
WEP 128 (104-bit key)	Select the *WEP 128 (104 bit key)* button to display the *WEP 128 Settings* field within the New Security Policy screen. For specific information on configuring WEP 128, see "Configuring WEP Encryption" on page 208.
KeyGuard	Select the *KeyGuard* button to display the *KeyGuard Settings* field within the New Security Policy screen. For specific information on configuring KeyGuard, see "Configuring KeyGuard Encryption" on page 209.
WPA/WPA2 TKIP	Select the *WPA/WPA2 TKIP* button to display the *WPA/TKIP Settings* field within the New Security Policy screen. For specific information on configuring WPA/WPA2 TKIP, see "Configuring WPA/WPA2 Using TKIP" on page 211.
WPA2/CCMP (802.11i)	Select the *WPA2/CCMP (802.11)* button to display the *WPA2/CCMP Settings* field within the New Security Policy screen. For detailed information on configuring WPA2/CCMP, see "Configuring WPA2-CCMP (802.11i)" on page 213.

6 Click *Apply* to keep changes made within the New Security Policy screen (if any).

Configure encryption or authentication supported security policies by referring to the following.

For access point authentication:

- To create a security policy supporting Kerberos, see, "Configuring Kerberos Authentication" on page 202.
- To define a security policy supporting 802.1x EAP, see "Configuring 802.1x EAP Authentication" on page 204.

For access point encryption:

- To create a security policy supporting WEP, see "Configuring WEP Encryption" on page 208.
- To define a security policy supporting KeyGuard, see, "Configuring KeyGuard Encryption" on page 209.
- To configure a security policy supporting WPA/TKIP, see "Configuring WPA/WPA2 Using TKIP" on page 211.
- To create a security policy supporting WPA2/CCMP, see "Configuring WPA2-CCMP (802.11i)" on page 213.

7 Click *Cancel* to return to the target WLAN screen without keeping any of the changes made within the New Security Policy screen.

Configuring Kerberos Authentication

Kerberos (designed and developed by MIT) provides strong authentication for client/server applications using secret-key cryptography. Using Kerberos, a client must prove its identity to a server (and vice versa) across an insecure network connection.

Once a client and server use Kerberos to prove their identity, they can encrypt all communications to assure privacy and data integrity. Kerberos can only be used on the Access Point with certain Motorola 802.11b clients.

CAUTION

Kerberos makes no provisions for host security. Kerberos assumes that it is running on a trusted host with an untrusted network. If host security is compromised, Kerberos is compromised as well

Kerberos uses the *Network Time Protocol (NTP)* for synchronizing the clocks of its *Key Distribution Center (KDC) server(s)*. Use the *NTP Servers* screen to specify the IP addresses and ports of available NTP servers. Kerberos requires the *Enable NTP on* checkbox be selected for authentication to function properly. See "Configuring Network Time Protocol (NTP)" on page 110 to configure the NTP server.

NOTE

If 802.11a/n is selected as the radio used for a specific WLAN, the WLAN cannot use a Kerberos supported security policy, as no Motorola 802.11a/n clients can support Kerberos.

To configure Kerberos on the access point:

1 Select *Network Configuration* > *Wireless* > *Security* from the access point menu tree.

If security policies supporting Kerberos exist, they appear within the *Security Configuration* screen. These existing policies can be used as is, or their properties edited by clicking the *Edit* button. To configure a new security policy supporting Kerberos, continue to step 2.

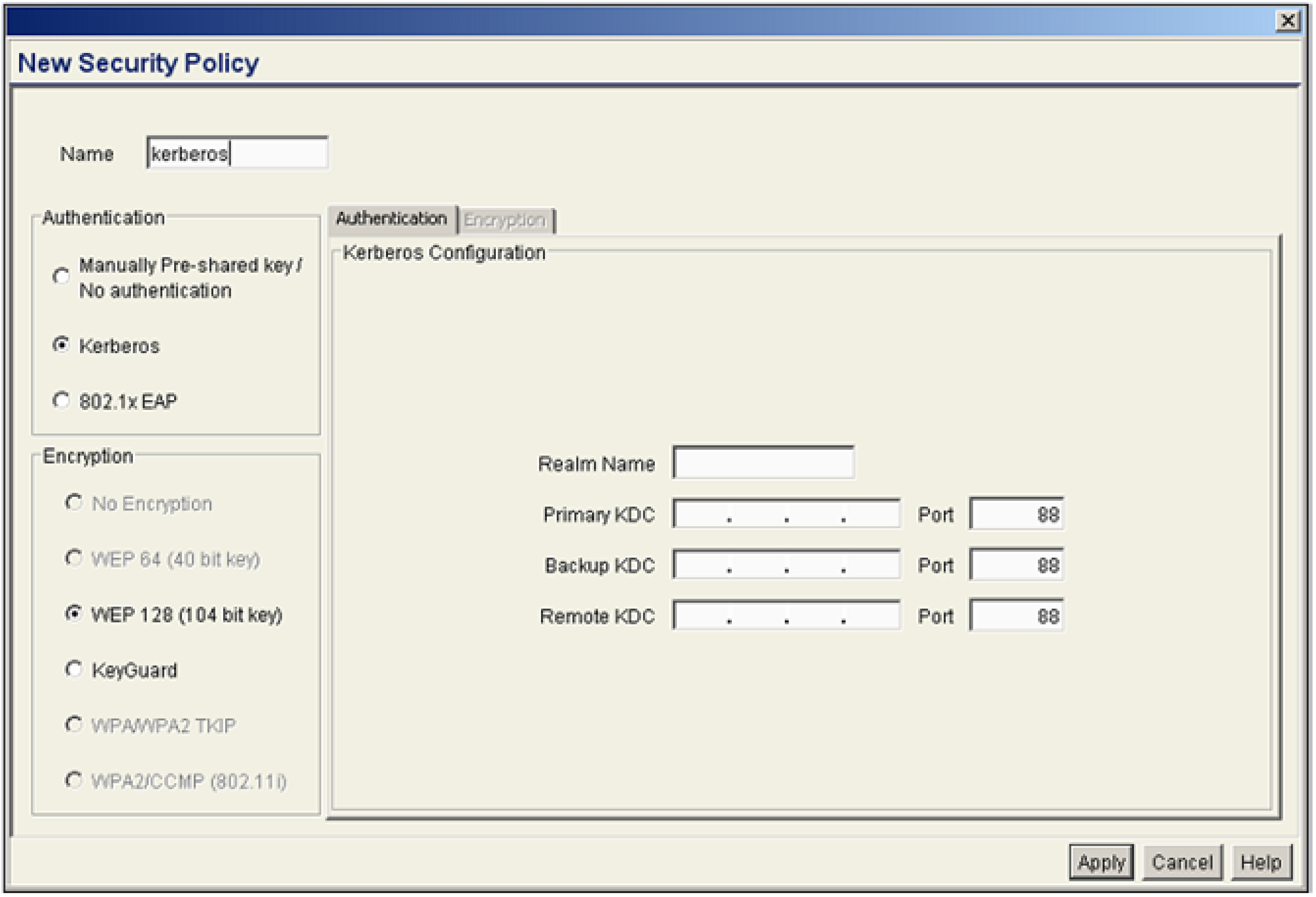
2 Click the *Create* button to configure a new policy supporting Kerberos.

The *New Security Policy* screen displays with no authentication or encryption options selected.

3 Select the *Kerberos* radio button.

The *Kerberos Configuration* field displays within the New Security Policy screen.

4 Ensure the *Name* of the security policy entered suits the intended configuration or function of the policy.



New Security Policy

Name: kerberos

Authentication
- ○ Manually Pre-shared key / No authentication
- ● Kerberos
- ○ 802.1x EAP

Encryption
- ○ No Encryption
- ○ WEP 64 (40 bit key)
- ● WEP 128 (104 bit key)
- ○ KeyGuard
- ○ WPA/WPA2 TKIP
- ○ WPA2/CCMP (802.11i)

Kerberos Configuration
- Realm Name:
- Primary KDC: . . . Port: 88
- Backup KDC: . . . Port: 88
- Remote KDC: . . . Port: 88

5 Set the *Kerberos Configuration* field as required to define the parameters of the Kerberos authentication server and access point.

Realm Name — Specify a realm name that is case-sensitive, for example, extremenetworks.com. The realm name is the name domain/realm name of the KDC Server. A realm name functions similarly to a DNS domain name. In theory, the realm name is arbitrary. However, in practice a Kerberos realm is named by uppercasing the DNS domain name that is associated with hosts in the realm.

Primary KDC — Specify a numerical (non-DNS) IP address and port for the primary *Key Distribution Center (KDC).* The KDC implements an Authentication Service and a Ticket Granting Service, whereby an authorized user is granted a ticket encrypted with the user's password. The KDC has a copy of every user password.

Backup KDC — Optionally, specify a numerical (non-DNS) IP address and port for a backup KDC. Backup KDCs are referred to as slave servers. The slave server periodically synchronizes its database with the primary (or master) KDC.

Remote KDC	Optionally, specify a numerical (non-DNS) IP address and port for a remote KDC. Kerberos implementations can use an administration server allowing remote manipulation of the Kerberos database. This administration server usually runs on the KDC.
Port	Specify the ports on which the Primary, Backup and Remote KDCs reside. The default port number for Kerberos Key Distribution Centers is Port 88.

6 Click the *Apply* button to return to the *WLAN* screen to save any changes made within the Kerberos Configuration field of the New Security Policy screen.

7 Click the *Cancel* button to undo any changes made within the Kerberos Configuration field and return to the *WLAN* screen. This reverts all settings for the Kerberos Configuration field to the last saved configuration.

Configuring 802.1x EAP Authentication

The IEEE 802.1x standard ties the 802.1x EAP authentication protocol to both wired and wireless LAN applications.

The EAP process begins when an unauthenticated supplicant (client device) tries to connect with an authenticator (in this case, the authentication server). The access point passes EAP packets from the client to an authentication server on the wired side of the access point. All other packet types are blocked until the authentication server (typically, a RADIUS server) verifies the MU’s identity.

To configure 802.1x EAP authentication on the access point:

1 Select *Network Configuration > Wireless > Security* from the access point menu tree.

If security policies supporting 802.1x EAP exist, they appear within the *Security Configuration* screen. These existing policies can be used as is, or their properties edited by clicking the *Edit* button. To configure a new security policy supporting 802.1x EAP, continue to step 2.

2 Click the *Create* button to configure a new policy supporting 802.1x EAP.

The *New Security Policy* screen displays with no authentication or encryption options selected.

3 Select the *802.1x EAP* radio button.

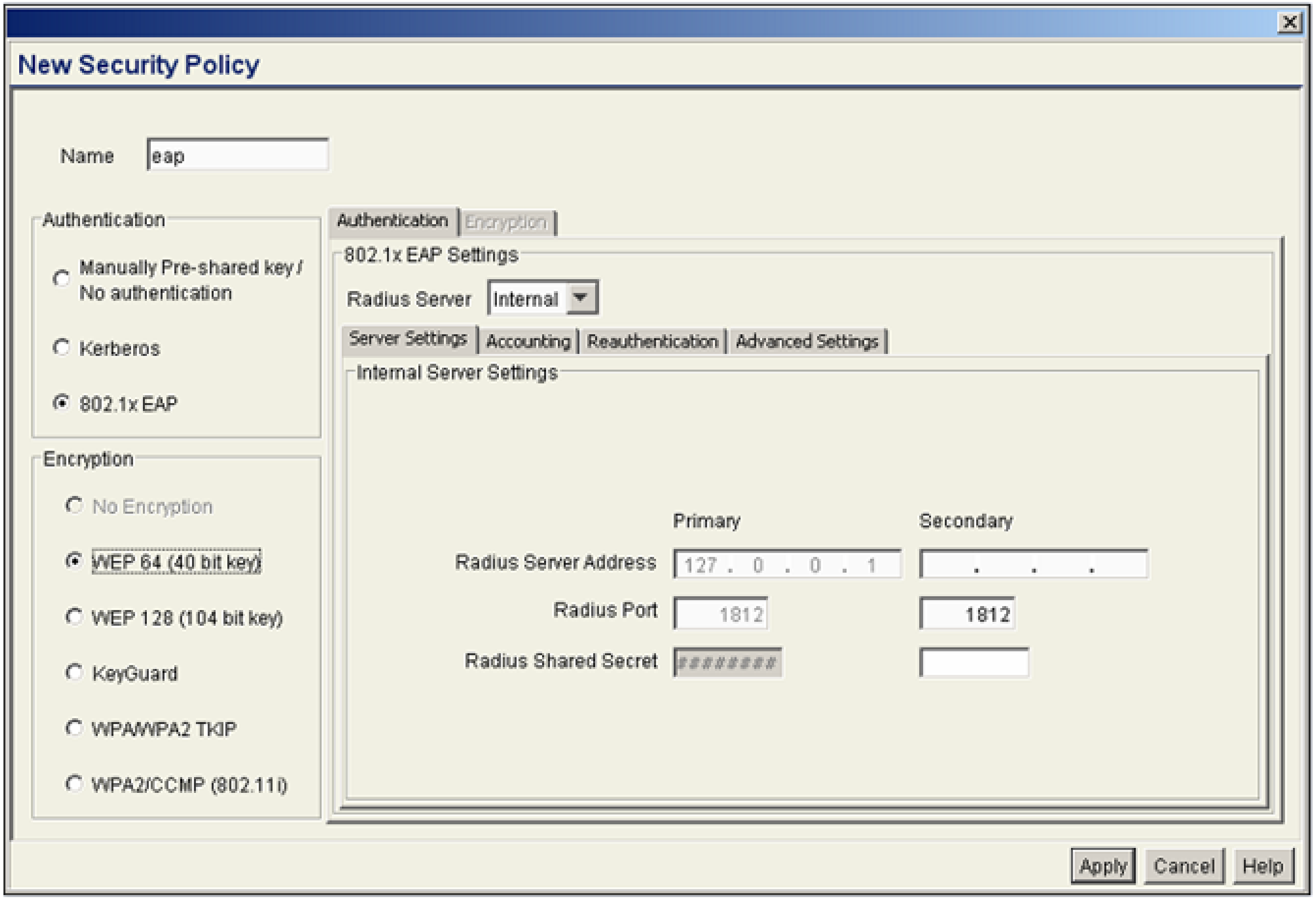
The *802.1x EAP Settings* field displays within the New Security Policy screen.

4 Ensure the *Name* of the security policy entered suits the intended configuration or function of the policy.

5 If using the Access Point’s Internal RADIUS server, leave the *Radius Server* drop-down menu in the default setting of *Internal*. If an external RADIUS server is used, select *External* from the drop-down menu.

CAUTION

If using external RADIUS authentication with admin users, and the connectivity to the RADIUS server is lost, the values will revert to local authentication.



New Security Policy

Name: eap

Authentication
○ Manually Pre-shared key / No authentication
○ Kerberos
● 802.1x EAP

Encryption
○ No Encryption
● WEP 64 (40 bit key)
○ WEP 128 (104 bit key)
○ KeyGuard
○ WPA/WPA2 TKIP
○ WPA2/CCMP (802.11i)

802.1x EAP Settings

Radius Server: Internal

Internal Server Settings

	Primary	Secondary
Radius Server Address	127 . 0 . 0 . 1	. . .
Radius Port	1812	1812
Radius Shared Secret	########	

6 Configure the *Server Settings* field as required to define address information for the authentication server. The appearance of the Server Settings field varies depending on whether Internal or External has been selected from the *Radius Server* drop-down menu.

Radius Server Address

If using an External RADIUS Server, specify the numerical (non-DNS) IP address of a primary *Remote Dial-In User Service* (RADIUS) server. Optionally, specify the IP address of a secondary server. The secondary server acts as a failover server if the primary server cannot be contacted. An ISP or a network administrator provides these addresses.

RADIUS is a client/server protocol and software enabling remote-access clients to communicate with a server used to authenticate users and authorize access to the requested system or service. This setting is not available if Internal has been selected from the RADIUS Server drop-down menu.

Radius Port

If using an External Radius Server, specify the port on which the primary Radius server is listening. Optionally, specify the port of a secondary (failover) server. Older Radius servers listen on ports 1645 and 1646. Newer servers listen on ports 1812 and 1813. Port 1645 or 1812 is used for authentication. Port 1646 or 1813 is used for accounting. The ISP or a network administrator needs to confirm the appropriate primary and secondary port numbers for authentication. This setting is not available if Internal has been selected from the Radius Server drop-down menu.

Radius Shared Secret

Specify a shared secret for authentication on the Internal or Primary RADIUS server (External RADIUS Server only). The shared secret is required to match the shared secret on the RADIUS server. Optionally, specify a shared secret for a secondary (failover) server. Use shared secrets to verify RADIUS messages (with the exception of the Access-Request message) sent by a RADIUS enabled device configured with the same shared secret.

Apply the qualifications of a well-chosen password to the generation of a shared secret. Generate a random, case-sensitive string using letters and numbers. Verify the shared secret is at least 22 characters to protect the RADIUS server from brute-force attacks. An example of a strong and secure shared secret is: 8d#>9fq4bV)H7%a3-zE13sW.

7 Select the *Accounting* tab as required to define a timeout period and retry interval Syslog for MUs interoperating with the access point and EAP authentication server. The items within this tab could be enabled or disabled depending on whether Internal or External has been selected from the RADIUS Server drop-down menu.

External Radius Server Address

Specify the IP address of the external RADIUS server used to provide RADIUS accounting.

External Radius Port

Specify the port on which the RADIUS server is listening. The default port is 1813.

External Radius Shared Secret

Specify a shared secret for authentication. The shared secret is required to match the shared secret on the RADIUS server.

MU Timeout

Specify the time (in seconds) for the Access Point’s retransmission of EAP-Request packets. The default is 10 seconds. If this time is exceeded, the authentication session is terminated.

Retries

Specify the number of retries for the MU to retransmit a missed frame to the RADIUS server before it times out of the authentication session. The default is 2 retries.

Enable Syslog

Select the *Enable Syslog* checkbox to enable RADIUS accounting syslog messages relating to EAP events to be written to the specified syslog server.

Syslog Server IP Address

Enter the IP address of the destination syslog server to be used to log EAP events.

8 Select the *Reauthentication* tab as required to define authentication connection policies, intervals and maximum retries. The items within this tab are identical regardless of whether Internal or External is selected from the RADIUS Server drop-down menu.

Enable Reauthentication

Select the *Enable Reauthentication* checkbox to configure a wireless connection policy so MUs are forced to reauthenticate periodically. Periodic repetition of the EAP process provides ongoing security for current authorized connections.

Period (30-9999) secs

Set the EAP reauthentication period to a shorter interval for tighter security on the WLAN's connections. Set the EAP reauthentication period to a longer time interval (at most, 9999 seconds) to relax security on wireless connections. The default interval of 3600 seconds is recommended.

Max. Retries (1-99) retries

Define the maximum number of MU retries to reauthenticate after failing to complete the EAP process. Failure to reauthenticate in the specified number of retries results in a terminated connection. The default is 2 retries.

NOTE

The default values described are the recommended values. Do not change these values unless consulted otherwise by an administrator.

9 Select the *Advanced Settings* tab as required to specify a MU quiet period, timeout interval, transmit period, and retry period for MUs and the authentication server. The items within this tab are identical regardless of whether Internal or External is selected from the RADIUS Server drop-down menu.

MU Quiet Period (1-65535) secs

Specify an idle time (in seconds) between MU authentication attempts, as required by the authentication server. The default is 10 seconds.

MU Timeout (1-255) secs

Define the time (in seconds) for the Access Point’s retransmission of EAP-Request packets. The default is 10 seconds.

MU Tx Period (1-65635) secs

Specify the time period (in seconds) for the Access Point's retransmission of the EAP Identity Request frame. The default is 5 seconds.

MU Max Retries (1-10) retries

Specify the maximum number of times the Access Point retransmits an EAP-Request frame to the client before it times out the authentication session. The default is 2 retries.

Server Timeout (1-255) secs

Specify the time (in seconds) for the Access Point's retransmission of EAP-Request packets to the server. The default is 5 seconds. If this time is exceeded, the authentication session is terminated.

Server Max Retries (1-255 retries)

Specify the maximum number of times for the Access Point to retransmit an EAP-Request frame to the server before it times out the authentication session. The default is 2 retries.

10 Click the *Apply* button to save any changes made within the 802.1x EAP Settings field (including all 5 selectable tabs) of the New Security Policy screen.

11 Click the *Cancel* button to undo any changes made within the 802.1x EAP Settings field and return to the *WLAN* screen. This reverts all settings for the 802.1x EAP Settings field to the last saved configuration.

Configuring WEP Encryption

Wired Equivalent Privacy (WEP) is a security protocol specified in the *IEEE Wireless Fidelity (Wi-Fi)* standard. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN.

WEP may be all that a small-business user needs for the simple encryption of wireless data. However, networks that require more security are at risk from a WEP flaw. The existing 802.11 standard alone offers administrators no effective method to update keys.

To configure WEP on the access point:

1 Select *Network Configuration* > *Wireless* > *Security* from the access point menu tree.

  If security policies supporting WEP exist, they appear within the *Security Configuration* screen. These existing policies can be used as is, or their properties edited by clicking the *Edit* button. To configure a new security policy supporting WEP, continue to step 2.

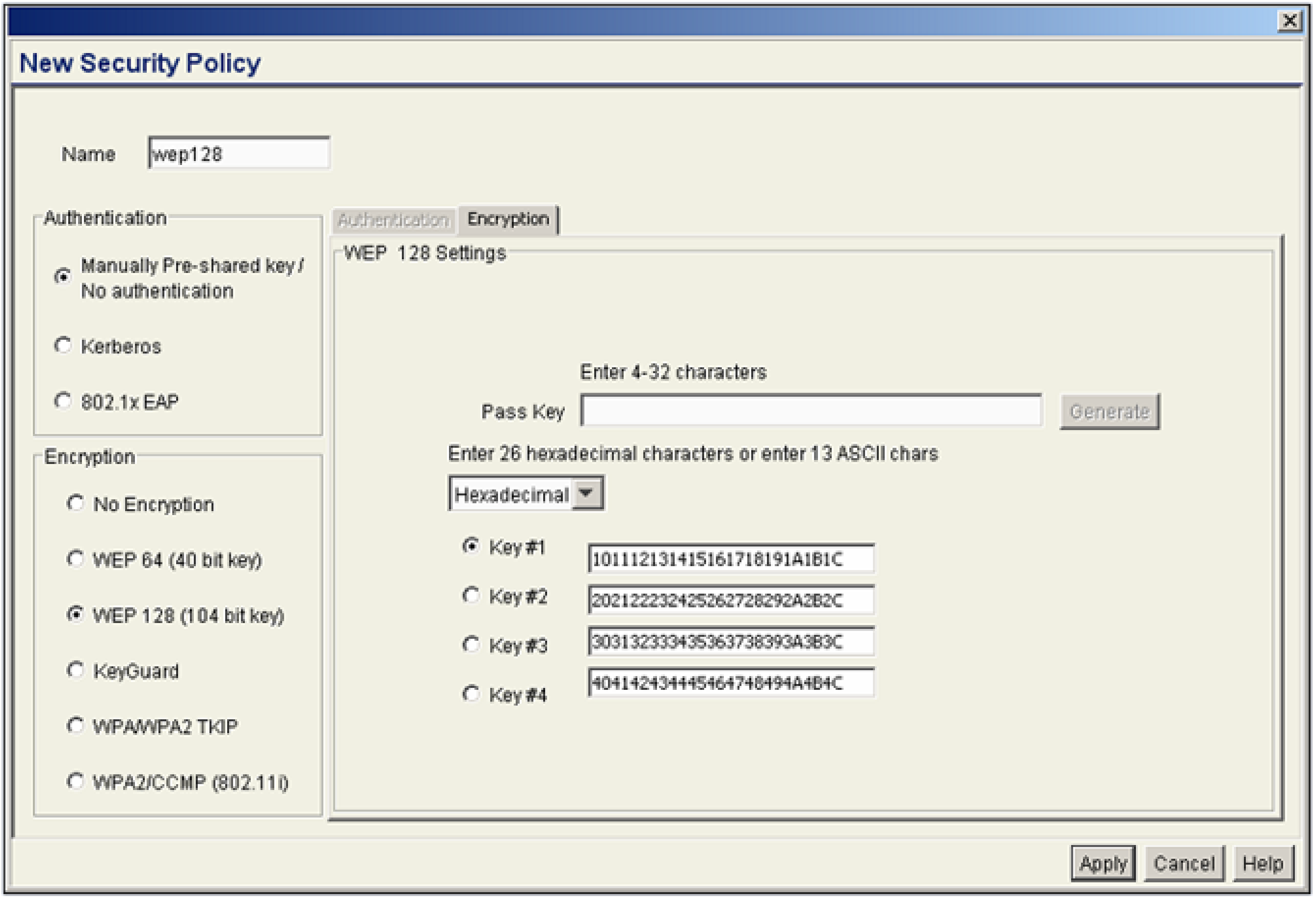
2 Click the *Create* button to configure a new policy supporting WEP.

  The *New Security Policy* screen displays with no authentication or encryption options selected.

3 Select either the *WEP 64 (40 bit key)* or *WEP 128 (104 bit key)* radio button.

  The *WEP 64 Settings* or *WEP 128 Settings* field displays within the New Security Policy screen.

4 Ensure the *Name* of the security policy entered suits the intended configuration or function of the policy.



New Security Policy

Name: wep128

Authentication
- ● Manually Pre-shared key / No authentication
- ○ Kerberos
- ○ 802.1x EAP

Encryption
- ○ No Encryption
- ○ WEP 64 (40 bit key)
- ● WEP 128 (104 bit key)
- ○ KeyGuard
- ○ WPA/WPA2 TKIP
- ○ WPA2/CCMP (802.11i)

WEP 128 Settings

Enter 4-32 characters

Pass Key:

Enter 26 hexadecimal characters or enter 13 ASCII chars

Hexadecimal

- ● Key #1 101112131415161718191A1B1C
- ○ Key #2 202122232425262728292A2B2C
- ○ Key #3 303132333435363738393A3B3C
- ○ Key #4 404142434445464748494A4B4C

5 Configure the *WEP 64 Settings* or *WEP 128 Settings* field as required to define the Pass Key used to generate the WEP keys. These keys must be the same between the Access Point and its MU to encrypt packets between the two devices.

Pass Key

Specify a 4 to 32 character pass key and click the *Generate* button. The pass key can be any alphanumeric string. The access point, other proprietary routers and Motorola MUs use the algorithm to convert a string to the same hexadecimal number. MUs without Motorola adapters need to use WEP keys manually configured as hexadecimal numbers.

Keys #1-4

Use the *Key #1-4* areas to specify key numbers. For WEP 64 (40-bit key), the keys are 10 hexadecimal characters in length. For WEP 128 (104-bit key), the keys are 26 hexadecimal characters in length. Select one of these keys for activation by clicking its radio button.

Default (hexadecimal) keys for WEP 64 include:

Key 1	1011121314
Key 2	2021222324
Key 3	3031323334
Key 4	4041424344

Default (hexadecimal) keys for WEP 128 include:

Key 1	101112131415161718191A1B1C
Key 2	202122232425262728292A2B2C
Key 3	303132333435363738393A3B3C
Key 4	404142434445464748494A4B4C

6 Click the *Apply* button to save any changes made within the WEP 64 Setting or WEP 128 Setting field of the New Security Policy screen.

7 Click the *Cancel* button to undo any changes made within the WEP 64 Setting or WEP 128 Setting field and return to the *WLAN* screen. This reverts all settings to the last saved configuration.

Configuring KeyGuard Encryption

KeyGuard is an enhancement to WEP encryption, and was developed before the finalization of WPA-TKIP. This encryption implementation is based on the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i.

WPA2-CCMP (not KeyGuard) offers the highest level of security among the encryption methods available with the access point.

1 Select *Network Configuration* > *Wireless* > *Security* from the access point menu tree.

If security policies supporting KeyGuard exist, they appear within the *Security Configuration* screen. These existing policies can be used as is, or their properties edited by clicking the *Edit* button. To configure a new security policy supporting KeyGuard, continue to step 2.

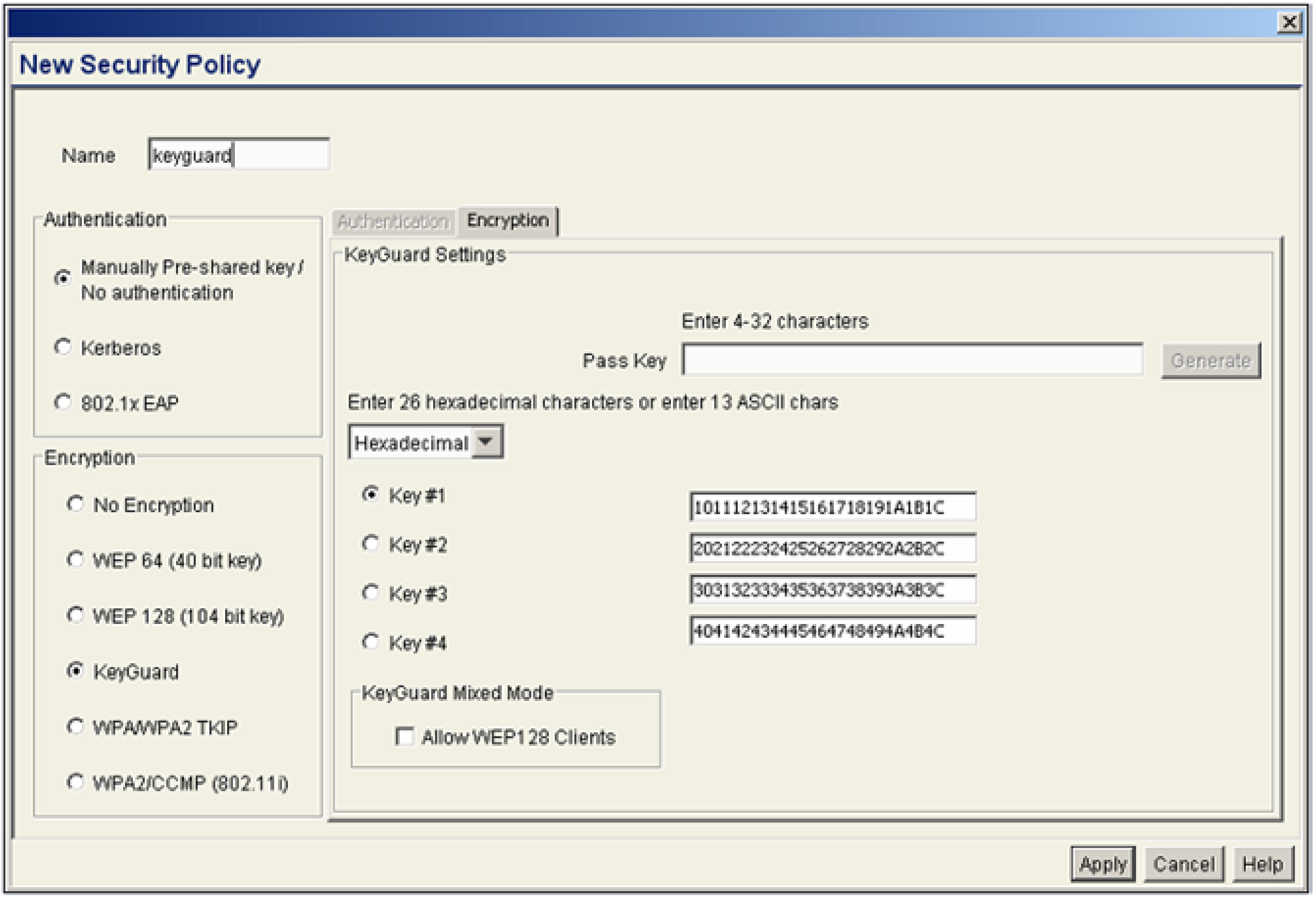
2 Click the *Create* button to configure a new policy supporting KeyGuard.

The *New Security Policy* screen displays with no authentication or encryption options selected.

3 Select the *KeyGuard* radio button.

The *KeyGuard Settings* field displays within the New Security Policy screen.

4 Ensure the *Name* of the security policy entered suits the intended configuration or function of the policy.



New Security Policy

Name: keyguard

Authentication

- ● Manually Pre-shared key / No authentication
- ○ Kerberos
- ○ 802.1x EAP

Encryption

- ○ No Encryption
- ○ WEP 64 (40 bit key)
- ○ WEP 128 (104 bit key)
- ● KeyGuard
- ○ WPA/WPA2 TKIP
- ○ WPA2/CCMP (802.11i)

KeyGuard Settings

Enter 4-32 characters

Pass Key:

Enter 26 hexadecimal characters or enter 13 ASCII chars

Hexadecimal

- ● Key #1: 101112131415161718191A1B1C
- ○ Key #2: 202122232425262728292A2B2C
- ○ Key #3: 303132333435363738393A3B3C
- ○ Key #4: 404142434445464748494A4B4C

KeyGuard Mixed Mode

□ Allow WEP128 Clients

5 Configure the *KeyGuard Settings* field as required to define the Pass Key used to generate the WEP keys used with the KeyGuard algorithm. These keys must be the same between the Access Point and its MU to encrypt packets between the two devices

Pass Key	Specify a 4 to 32 character pass key and click the *Generate* button. The pass key can be any alphanumeric string. The access point, other proprietary routers, and Motorola MUs use the algorithm to convert a string to the same hexadecimal number. MUs without Motorola adapters need to use WEP keys manually configured as hexadecimal numbers.
Keys #1-4	Use the *Key #1-4* areas to specify key numbers. The keys are 26 hexadecimal characters in length. Select one of these keys for activation by clicking its radio button.

Default (hexadecimal) keys for KeyGuard include:

Key 1	101112131415161718191A1B1C
Key 2	202122232425262728292A2B2C
Key 3	303132333435363738393A3B3C

Key 4	404142434445464748494A4B4C

6 Select the *Allow WEP128 Clients* checkbox (from within the *KeyGuard Mixed Mode* field) to enable WEP128 clients to associate with an Access Point's KeyGuard supported WLAN. The WEP128 clients must use the same keys as the KeyGuard clients to interoperate within the Access Point's KeyGuard supported WLAN.

7 Click the *Apply* button to save any changes made within the KeyGuard Setting field of the New Security Policy screen.

8 Click the *Cancel* button to undo any changes made within the KeyGuard Setting field and return to the *WLAN* screen. This reverts all settings to the last saved configuration.

Configuring WPA/WPA2 Using TKIP

Wi-Fi Protected Access (WPA) is a robust encryption scheme specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i. WPA provides more sophisticated data encryption than WEP. WPA is designed for corporate networks and small-business environments where more wireless traffic allows quicker discovery of encryption keys by an unauthorized person.

The encryption method is *Temporal Key Integrity Protocol (TKIP).* TKIP addresses WEP's weaknesses with a re-keying mechanism, a per-packet mixing function, a message integrity check, and an extended initialization vector.

Wi-Fi Protected Access 2 (WPA2) is an enhanced version of WPA. WPA2 uses the *Advanced Encryption Standard* (AES) instead of TKIP. AES supports 128-bit, 192-bit and 256-bit keys.

WPA/WPA2 also provide strong user authentication based on 802.1x EAP. To configure WPA/WPA2 encryption on the access point:

1 Select *Network Configuration* > *Wireless* > *Security* from the access point menu tree.

If security policies supporting WPA-TKIP exist, they appear within the *Security Configuration* screen. These existing policies can be used as is, or their properties edited by clicking the *Edit* button. To configure a new security policy supporting WPA-TKIP, continue to step 2.

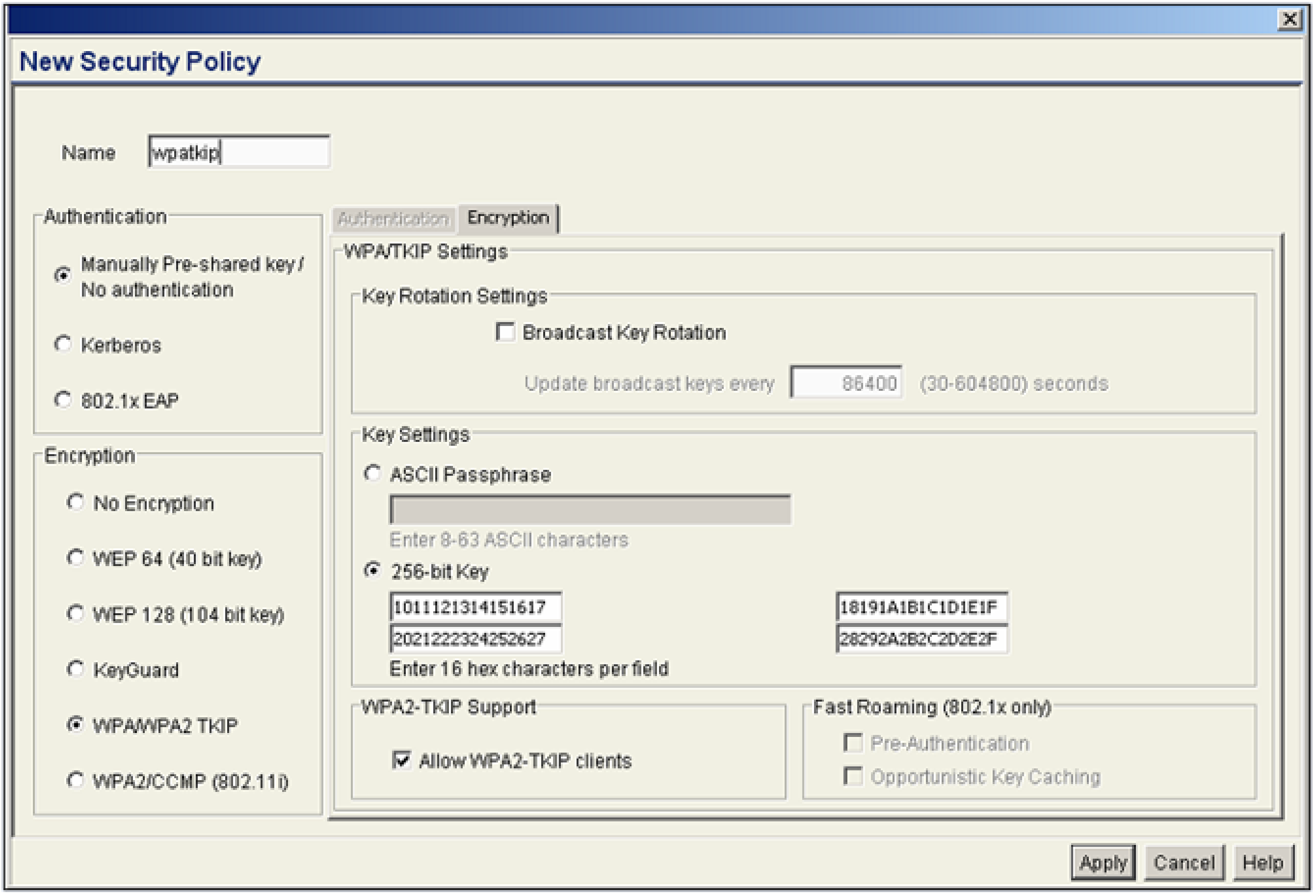
2 Click the *Create* button to configure a new policy supporting WPA-TKIP.

The *New Security Policy* screen displays with no authentication or encryption options selected.

3 Select the *WPA/WPA2 TKIP* radio button.

The *WPA/TKIP Settings* field displays within the New Security Policy screen.

4 Ensure the *Name* of the security policy entered suits the intended configuration or function of the policy.



Name: wpatkip

Authentication

● Manually Pre-shared key / No authentication

○ Kerberos

○ 802.1x EAP

Encryption

○ No Encryption

○ WEP 64 (40 bit key)

○ WEP 128 (104 bit key)

○ KeyGuard

● WPA/WPA2 TKIP

○ WPA2/CCMP (802.11i)

WPA/TKIP Settings

Key Rotation Settings

□ Broadcast Key Rotation

Update broadcast keys every 86400 (30-604800) seconds

Key Settings

○ ASCII Passphrase

Enter 8-63 ASCII characters

● 256-bit Key

1011121314151617	18191A1B1C1D1E1F
2021222324252627	28292A2B2C2D2E2F

Enter 16 hex characters per field

WPA2-TKIP Support

☑ Allow WPA2-TKIP clients

Fast Roaming (802.1x only)

□ Pre-Authentication

□ Opportunistic Key Caching

5 Configure the *Key Rotation Settings* area as needed to broadcast encryption key changes to MUs and define the broadcast interval.

Broadcast Key Rotation	Select the *Broadcast Key Rotation* checkbox to enable or disable broadcast key rotation. When enabled, the key indices used for encrypting/decrypting broadcast traffic will be alternatively rotated on every interval specified in the Broadcast Key Rotation Interval. Enabling broadcast key rotation enhances the broadcast traffic security on the WLAN. This value is disabled by default.
Update broadcast keys every (300-604800 seconds)	Specify a time period in seconds to rotate the key index used for the broadcast key. Set the interval to a shorter duration like 3600 seconds for tighter broadcast traffic security on the wireless LAN. Set the interval to a longer duration like 86400 seconds for less broadcast traffic security requirements. Default value is 86400 secs.

6 Configure the *Key Settings* area as needed to set an ASCII Passphrase and key values.

ASCII Passphrase	To use an ASCII passphrase (and not a hexadecimal value), select the checkbox and enter an alphanumeric string of 8 to 63 characters. The alphanumeric string allows character spaces. The access point converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

256-bit Key	To use a hexadecimal value (and not an ASCII passphrase), select the checkbox and enter 16 hexadecimal characters into each of the four fields displayed.

Default (hexadecimal) 256-bit keys for WPA/TKIP include:

- 1011121314151617
- 18191A1B1C1D1E1F
- 2021222324252627
- 28292A2B2C2D2E2F

7 Enable *WPA2-TKIP Support* as needed to allow WPA2 and TKIP client interoperation.

Allow WPA2-TKIP clients	WPA2-TKIP support enables WPA2 and TKIP clients to operate together on the network.

8 Configure the *Fast Roaming (802.1x only)* field as required to enable additional access point roaming and key caching options. This feature is applicable only when using 802.1x EAP authentication with WPA2-TKIP.

Pre-Authentication	Selecting this option enables an associated MU to carry out an 802.1x authentication with another access point before it roams to it. The access point caches the keying information of the client until it roams to the other access point. This enables the roaming client to start sending and receiving data sooner by not having to do 802.1x authentication after it roams. This feature is only supported when 802.1x EAP authentication and WPA2-TKIP is enabled.
Opportunistic PMK Caching	Select the *Opportunistic Pairwise Master Key* (PMK) Caching option to reduce handoff latency by pre-establishing security associations between an MU and the AP4700 Access Points in a wireless network.

NOTE

PMK key caching is enabled internally by default for WPA2-TKIP when 802.1x EAP authentication is enabled.

9 Click the *Apply* button to save any changes made within this New Security Policy screen.

10 Click the *Cancel* button to undo any changes made within the WPA/TKIP Settings field and return to the *WLAN* screen. This reverts all settings to the last saved configuration.

Configuring WPA2-CCMP (802.11i)

WPA2 is a newer 802.11i standard that provides even stronger wireless security than Wi-Fi Protected Access (WPA) and WEP. CCMP is the security standard used by the *Advanced Encryption Standard (AES).* AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check (MIC)* using the proven *Cipher Block Chaining (CBC)* technique. Changing just one bit in a message produces a totally different result.

WPA2/CCMP is based on the concept of a *Robust Security Network (RSN)*, which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the keys the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is an encryption scheme as secure as any the access point provides.

To configure WPA2-CCMP on the access point:

1 Select *Network Configuration* > *Wireless* > *Security* from the access point menu tree.

If security policies supporting WPA2-CCMP exist, they appear within the *Security Configuration* screen. These existing policies can be used as is, or their properties edited by clicking the *Edit* button. To configure a new security policy supporting WPA2-CCMP, continue to step 2.

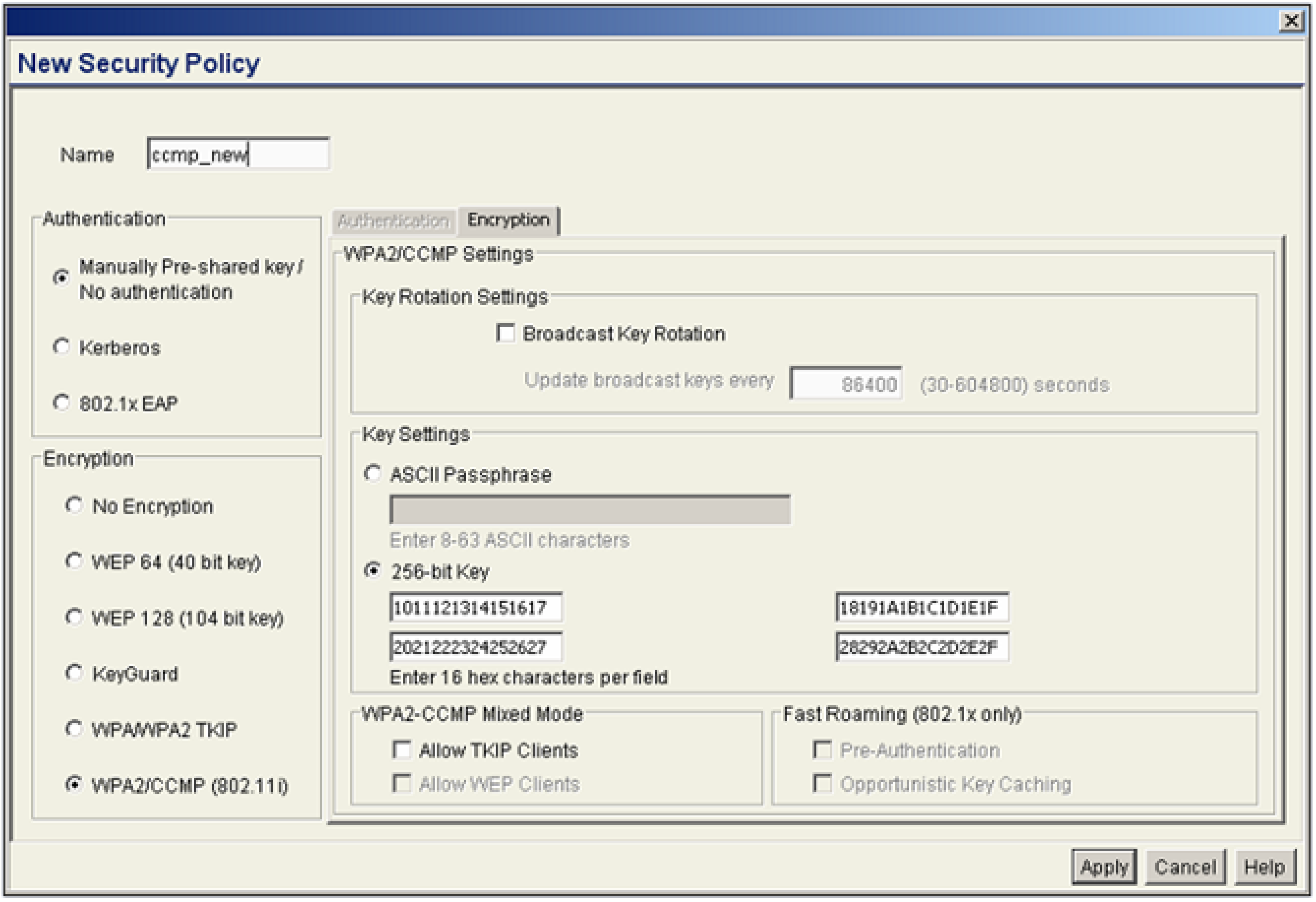
2 Click the *Create* button to configure a new policy supporting WPA2-CCMP.

The *New Security Policy* screen displays with no authentication or encryption options selected.

3 Select the *WPA2/CCMP (802.11i)* checkbox.

The *WPA2/CCMP Settings* field displays within the New Security Policy screen.

4 Ensure the *Name* of the security policy entered suits the intended configuration or function of the policy.



New Security Policy

Name: ccmp_new

Authentication

● Manually Pre-shared key / No authentication
○ Kerberos
○ 802.1x EAP

Encryption

○ No Encryption
○ WEP 64 (40 bit key)
○ WEP 128 (104 bit key)
○ KeyGuard
○ WPA/WPA2 TKIP
● WPA2/CCMP (802.11i)

WPA2/CCMP Settings

Key Rotation Settings

□ Broadcast Key Rotation

Update broadcast keys every 86400 (30-604800) seconds

Key Settings

○ ASCII Passphrase

Enter 8-63 ASCII characters

● 256-bit Key

1011121314151617	18191A1B1C1D1E1F
2021222324252627	28292A2B2C2D2E2F

Enter 16 hex characters per field

WPA2-CCMP Mixed Mode

□ Allow TKIP Clients
□ Allow WEP Clients

Fast Roaming (802.1x only)

□ Pre-Authentication
□ Opportunistic Key Caching

5 Configure the *Key Rotation Settings* field as required to set Broadcast Key Rotation and the update interval.

Broadcast Key Rotation

Select the *Broadcast Key Rotation* checkbox to enable or disable broadcast key rotation. When enabled, the key indices used for encrypting/decrypting broadcast traffic will be alternatively rotated on every interval specified in the Broadcast Key Rotation Interval. Enabling broadcast key rotation enhances the broadcast traffic security on the WLAN. This value is disabled by default.

Update broadcast keys every (300-604800 seconds)

Specify a time period in seconds to rotate the key index used for the broadcast key. Set the interval to a shorter duration like 3600 seconds for tighter broadcast traffic security on the wireless LAN. Set the interval to a longer duration like 86400 seconds for less broadcast traffic security requirements. Default value is 86400 secs.

6 Configure the *Key Settings* area as needed to set an ASCII Passphrase and 128-bit key.

ASCII Passphrase

To use an ASCII passphrase (and not a hexadecimal value), select the checkbox enter an alphanumeric string of 8 to 63 characters. The string allows character spaces. The access point converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

256-bit Key

To use a hexadecimal value (and not an ASCII passphrase), select the checkbox and enter 16 hexadecimal characters into each of the four fields displayed.

Default (hexadecimal) 256-bit keys for WP2A/CCMP include:

- 1011121314151617
- 18191A1B1C1D1E1F
- 2021222324252627
- 28292A2B2C2D2E2F

7 Configure the *WPA2-CCMP Mixed Mode* field as needed to allow WPA and WPA2 TKIP client interoperation.

Allow WPA/WPA2-TKIP clients

WPA2-CCMP Mixed Mode enables WPA2-CCMP, WPA-TKIP and WPA2-TKIP clients to operate together on the network. Enabling this option allows backwards compatibility for clients that support WPA-TKIP and WPA2-TKIP but do not support WPA2-CCMP. Extreme Networks recommends enabling this feature if WPA-TKIP or WPA2-TKIP supported MUs operate within a WLAN populated by WPA2-CCMP enabled clients.

Allow WEP clients

WPA2-CCMP Mixed Mode enables WPA2-CCMP and WEP clients to operate together on the network.

8 Configure the *Fast Roaming (802.1x only)* field as required to enable additional access point roaming and key caching options.

Pre-Authentication

Selecting this option enables an associated MU to carry out an 802.1x authentication with another access point before it roams to it. The access point caches the keying information of the client until it roams to the other access point. This enables the roaming client to start sending and receiving data sooner by not having to do 802.1x authentication after it roams. This feature is only supported when 802.1x EAP authentication is enabled.

Opportunistic PMK Caching	Select the *Opportunistic Pairwise Master Key* (PMK) Caching option to reduce handoff latency by pre-establishing security associations between an MU and the AP4700 Access Points in the wireless network.

NOTE

PMK key caching is enabled internally by default when 802.1x EAP authentication is enabled.

9 Click the *Apply* button to save any changes made within this New Security Policy screen.

10 Click the *Cancel* button to undo any changes made within the WPA2/CCMP Settings field and return to the *WLAN* screen. This reverts all settings to the last saved configuration.

Configuring Multi Cipher Support

The Access Point's Multi Cipher allows legacy and new MUs (Wi-Fi handheld devices) within the same WLAN. Multi cipher extends the Access Point's existing WLAN security options by allowing dynamic WEP and 802.11i configurations to co-exist, and allowing multiple security policies to be associated with the same ESSID on different WLANs. Within such an environment, legacy MUs are capable of WEP, while new MUs are capable of WPA/2-TKIP and WPA2-CCMP encryption. This particular form of multi cipher (security) support helps maintain the co-existence of Dynamic WEP and 802.11i based environments.

To support this feature, certain security policy combinations need to be available on a per-WLAN basis. The following combinations are supported:

- WEP 64 and WPA/WPA2-TKIP
- WEP 64 and WPA2-CCMP
- WEP 128 and WPA/WPA2-TKIP
- WEP 128 and WPA2-CCMP
- WPA2-CCMP and WPA/WPA2-TKIP

To configure multi cipher support, WLANs should be created with the same ESSID, but different BSSIDs and security schemes. This results in the AP announcing different beacons for the same ESSID. MUs can then select a corresponding BSSID to associate, depending on their individual configurations.

From the MU's point of view, the scenario is as if there are two APs available with same ESSID, but different security policies. The MU can choose an appropriate AP based on its configuration.

NOTE

Multi Cipher is supported in adaptive mode (AAP), provided the required configuration is allowed on the controller.

Configuring multi cipher support requires:

- Creating WLANs with the same ESSID, but different BSSIDs and security schemes. This results in the AP beaconing the same ESSID, but a different BSSID.

- Each WLAN having a unique WLAN name. If a WLAN's name is same as the ESSID, it's difficult to distinguish them when doing WLAN-BSSID grouping.
- Not using WLANs with same ESSID and security scheme. If this were to be deployed, beacons will contain the same ESSID and security scheme data, but different BSSIDs would be generated, potentially confusing MUs.
- Ensuring WLANs with the same ESSID use the same authentication method(s) in their security policies.
- WLANs with the same ESSID not use both WEP64 and WEP128 as security schemes. If both are defined for the same ESSID, MUs configured with WEP could be associated with the wrong WLAN and fail to get an IP address.

NOTE

Since the AP supports a maximum of 4 different BSSID groups, Extreme Networks recommends grouping WLANs with common security schemes under the same BSSID group to support a greater number of WLANs.

To configure multiple cipher support:

1 Create a WLAN supporting WEP64 as its security scheme.

For information on how to create or edit a WLAN and assign it a security scheme, see "Creating/ Editing Individual WLANs" on page 148.

For information on how to assign a WLAN a security policy supporting WEP, see "Configuring WEP Encryption" on page 208.

2 Create a second WLAN with the same ESSID as the WLAN created in step 1. However, assign the second WLAN a security policy supporting WPA2-CCMP.

For information on how to assign a WLAN a security policy supporting WEP, see "Configuring WPA2-CCMP (802.11i)" on page 213.

NOTE

Ensure the WLANs created in steps 1 and 2 have unique names assigned.

3 Map the WLANs created in steps 1 and 2 to different BSSID groups.

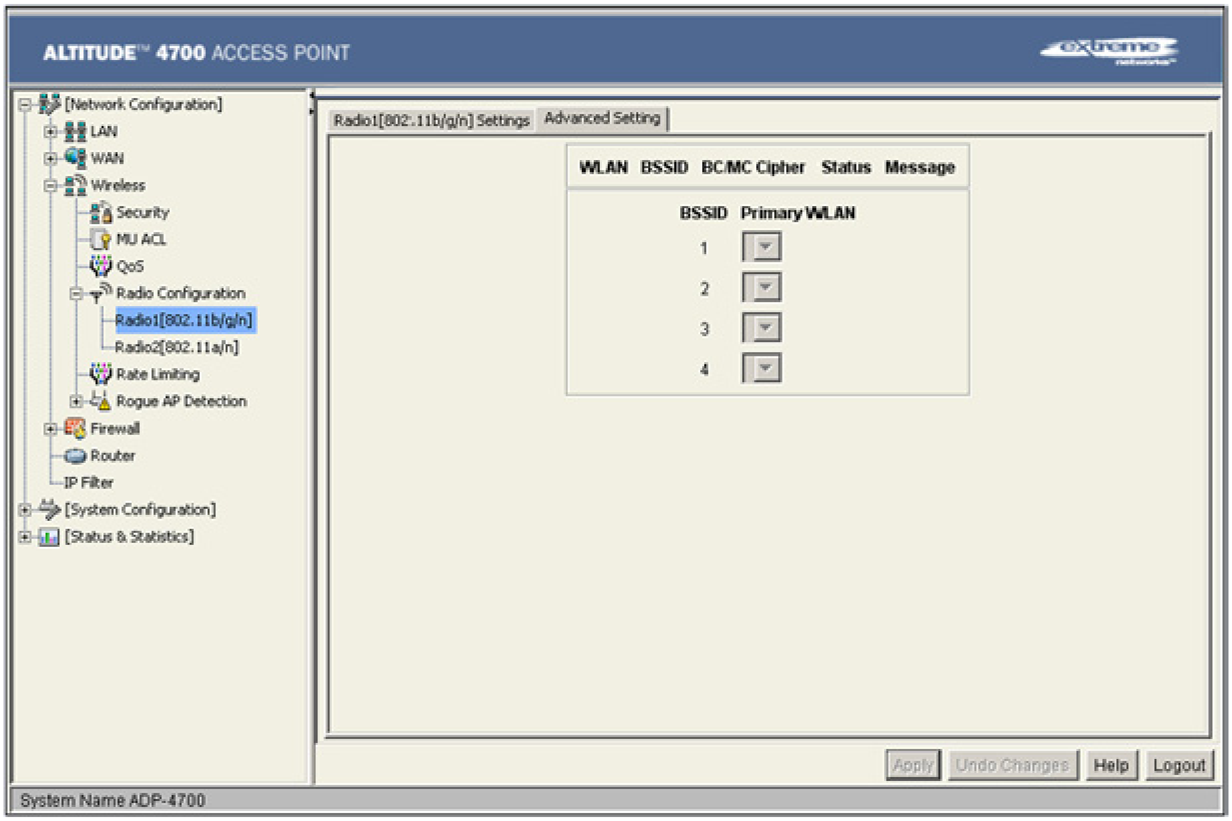
a Select *Network Configuration* > *Wireless* > *Radio Configuration* > *Radio1 or Radio 2* from the Access Point's menu tree.

b Select the *Advanced Settings* tab.

c MAP BSSIDs (4 BSSIDs are available for mapping) to WLANs. For additional information on how to MAP BSSIDs to WLANs, see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174.

CAUTION

When WLANs with WEP64/WEP128/TKIP/CCMP cipher suites are in the same BSSID group, a common cipher for the group encryption key cannot be set. Extreme Networks recommends grouping WLANs strategically into different BSSID groups. The status field in the WLAN-BSSID group mapping displays whether the WLANs in a particular BSSID group are up or not.



WLAN	BSSID	BC/MC Cipher	Status	Message

BSSID	Primary WLAN
1	
2	
3	
4	

This results in the AP beaconing the same ESSID but different WLAN BSSIDs and security schemes.

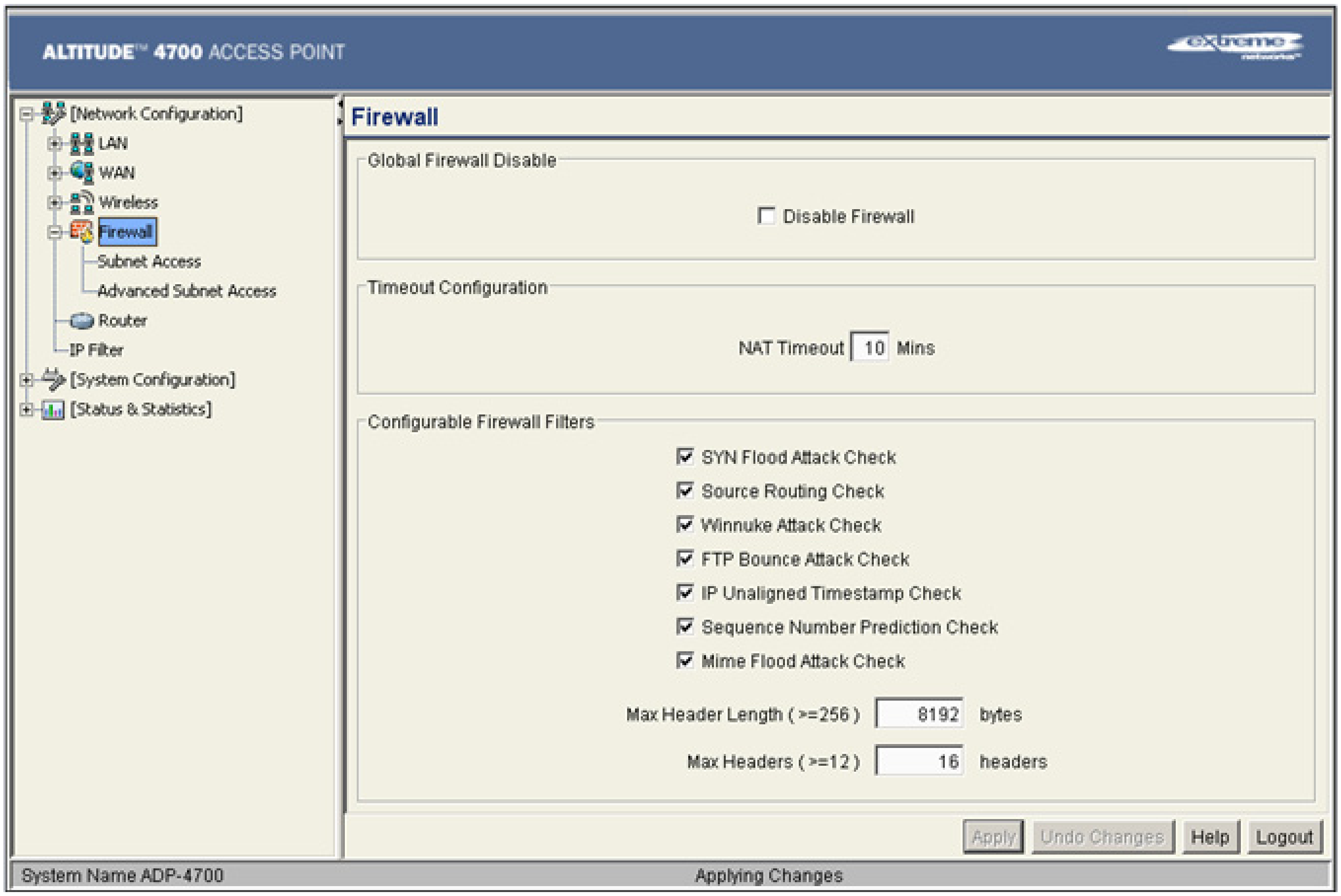
Configuring Firewall Settings

The access point's firewall is a set of related programs located in the gateway on the WAN side of the access point. The firewall uses a collection of filters to screen information packets for known types of system attacks. Some of the access point's filters are continuously enabled, others are configurable.

Use the access point’s *Firewall* screen to enable or disable the configurable firewall filters. Enable each filter for maximum security. Disable a filter if the corresponding attack does not seem a threat in order to reduce processor overhead. Use the WLAN Security screens (WEP, Kerberos etc.) as required for setting user authentication and data encryption parameters.

To configure the access point firewall settings:

1 Select *Network Configuration* > *Firewall* from the access point menu tree.



Firewall

Global Firewall Disable

☐ Disable Firewall

Timeout Configuration

NAT Timeout 10 Mins

Configurable Firewall Filters

☑ SYN Flood Attack Check
☑ Source Routing Check
☑ Winnuke Attack Check
☑ FTP Bounce Attack Check
☑ IP Unaligned Timestamp Check
☑ Sequence Number Prediction Check
☑ Mime Flood Attack Check

Max Header Length (>=256) 8192 bytes

Max Headers (>=12) 16 headers

System Name ADP-4700

Applying Changes

2 Refer to the *Global Firewall Disable* field to enable or disable the access point firewall.

Disable Firewall

Select the *Disable Firewall* checkbox to disable all firewall functions on the access point. This includes firewall filters, NAT, VP, content filtering, and subnet access. Disabling the access point firewall makes the access point vulnerable to data attacks and is not recommended during normal operation if using the WAN port.

3 Refer to the *Timeout Configuration* field to define a timeout interval to terminate IP address translations.

NAT Timeout

Network Address Translation (NAT) converts an IP address in one network to a different IP address or set of IP addresses in a different network. Set a *NAT Timeout* interval (in minutes) the access point uses to terminate the IP address translation process if no translation activity is detected after the specified interval.

4. Refer to the *Configurable Firewall Filters* field to set the following firewall filters:

   SYN Flood Attack Check
   A SYN flood attack requests a connection and then fails to promptly acknowledge a destination host's response, leaving the destination host vulnerable to a flood of connection requests.

   Source Routing Check
   A source routing attack specifies an exact route for a packet's travel through a network, while exploiting the use of an intermediate host to gain access to a private host.

   Winnuke Attack Check
   A "Win-nuking" attack uses the IP address of a destination host to send junk packets to its receiving port.

   FTP Bounce Attack Check
   An FTP bounce attack uses the PORT command in FTP mode to gain access to arbitrary ports on machines other than the originating client.

   IP Unaligned Timestamp Check
   An IP unaligned timestamp attack uses a frame with the IP timestamp option, where the timestamp is not aligned on a 32-bit boundary.

   Sequence Number Prediction Check
   A sequence number prediction attack establishes a three-way TCP connection with a forged source address. The attacker guesses the sequence number of the destination host response.

   Mime Flood Attack Check
   A MIME flood attack uses an improperly formatted MIME header in “sendmail” to cause a buffer overflow on the destination host.

   Max Header Length (>=256)
   Use the *Max Header Length* field to set the maximum allowable header length (at least 256 bytes).

   Max Headers (>=12)
   Use the *Max Headers* field to set the maximum number of headers allowed (at least 12 headers).

5. Click *Apply* to save any changes to the Firewall screen. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.
6. Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Firewall screen to the last saved configuration.
7. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

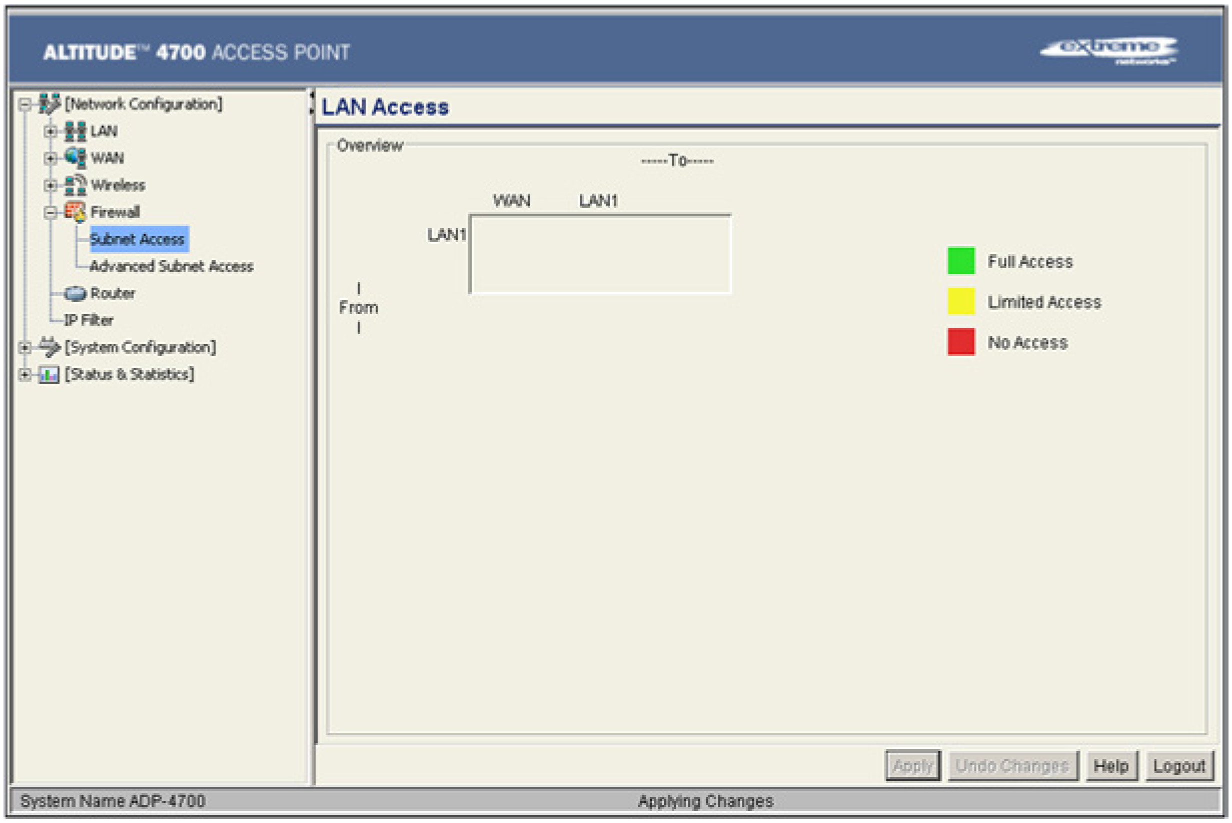
Configuring LAN to WAN Access

The access point LAN can be configured to communicate with the WAN side of the access point. Use the *Subnet Access* screen to control access from the LAN1 (or LAN2) interfaces to the WAN interface. This access level functions as an ACL in a router to allow/deny IP addresses or subnets to access certain interfaces (or subnets belonging to those interfaces) by creating access policies. It also functions as a filter to allow/deny access for certain protocols such as HTTP, Telnet, FTP etc.

To configure access point subnet access:

1. Select *Network Configuration > Firewall > Subnet Access* from the access point menu tree.
2. Refer to the *Overview* field to view rectangles representing subnet associations. The three possible colors indicate the current access level, as defined, for each subnet association.

Color	Access Type	Description
Green	Full Access	No protocol exceptions (rules) are specified. All traffic may pass between these two areas.
Yellow	Limited Access	One or more protocol rules are specified. Specific protocols are either enabled or disabled between these two areas. Click the table cell of interest and look at the exceptions area in the lower half of the screen to determine the protocols that are either allowed or denied.
Red	No Access	All protocols are denied, without exception. No traffic will pass between these two areas.



3 Configure the *Rules* field as required to allow or deny access to selected (enabled) protocols.

Allow or Deny all protocols, except	Use the drop-down menu to select either *Allow* or *Deny.* The selected setting applies to all protocols except those with enabled checkboxes and any traffic that is added to the table. For example, if the adoption rule is to Deny access to all protocols except those listed, access is allowed only to those selected protocols.

Pre configured Rules

The following protocols are preconfigured with the access point. To enable a protocol, check the box next to the protocol name.

- *HTTP—Hypertext Transfer Protocol* is the protocol for transferring files on the Web. HTTP is an application protocol running on top of the TCP/IP suite of protocols, the foundation protocols for the Internet. The HTTP protocol uses TCP port 80.
- *TELNET*—TELNET is the terminal emulation protocol of TCP/IP. TELNET uses TCP to achieve a virtual connection between server and client, then negotiates options on both sides of the connection. TELNET uses TCP port 23.
- *FTP—File Transfer Protocol (FTP)* is an application protocol using the Internet's TCP/IP protocols. FTP provides an efficient way to exchange files between computers on the Internet. FTP uses TCP port 21.
- *SMTP—Simple Mail Transfer Protocol* is a TCP/IP protocol for sending and receiving email. Due to its limited ability to queue messages at the receiving end, SMTP is often used with POP3 or IMAP. SMTP sends the email, and POP3 or IMAP receives the email. SMTP uses TCP port 25.
- *POP—Post Office Protocol* is a TCP/IP protocol intended to permit a workstation to dynamically access a maildrop on a server host. A workstation uses POP3 to retrieve email that the server is holding for it.
- *DNS—Domain Name Service* protocol searches for resources using a database distributed among different name servers.

Add

Click *Add* to create a new table entry.

Del (Delete)

Click *Del (Delete)* to remove a selected list entry.

Name

Specify a name for a newly configured protocol.

Transport

Select a protocol from the drop-down menu. For a detailed description of the protocols available, see “Available Protocols” on page 223.

Start Port

Enter the starting port number for a range of ports. If the protocol uses a single port, enter that port in this field.

End Port

Enter the ending port number for a port range. If the protocol uses a single port, leave the field blank. A new entry might use *Web Traffic* for its name, *TCP* for its protocol, and *80* for its port number.

4 Click *Apply* to save any changes to the Subnet Access screen. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.

5 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Subnet Access screen to the last saved configuration.

6 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Available Protocols

Protocols that are not pre-configured can be specified using the drop down list within the *Transport* column within the Subnet Access and Advanced Subnet Access screens. They include:

- *ALL*—Enables all of the protocol options displayed in the drop-down menu (as described below).
- *TCP—Transmission Control Protocol* is a set of rules for sending data as message units over the Internet. TCP manages individual data packets. Messages are divided into packets for efficient routing through the Internet.
- *UDP*—*User Datagram Protocol* is used for broadcasting data over the Internet. Like TCP, UDP runs on top of Internet Protocol (IP) networks. Unlike TCP/IP, UDP/IP provides few error recovery services. UDP offers a way to directly connect, and then send and receive datagrams over an IP network.
- *ICMP*—*Internet Control Message Protocol* is tightly integrated with IP. ICMP messages are used for out-of-band messages related to network operation. ICMP packet delivery is unreliable. Hosts cannot count on receiving ICMP packets for a network problem.
- *AH*—Authentication Header is one of the two key components of *IP Security Protocol* (IPsec). The other key component is *Encapsulating Security Protocol (ESP).*

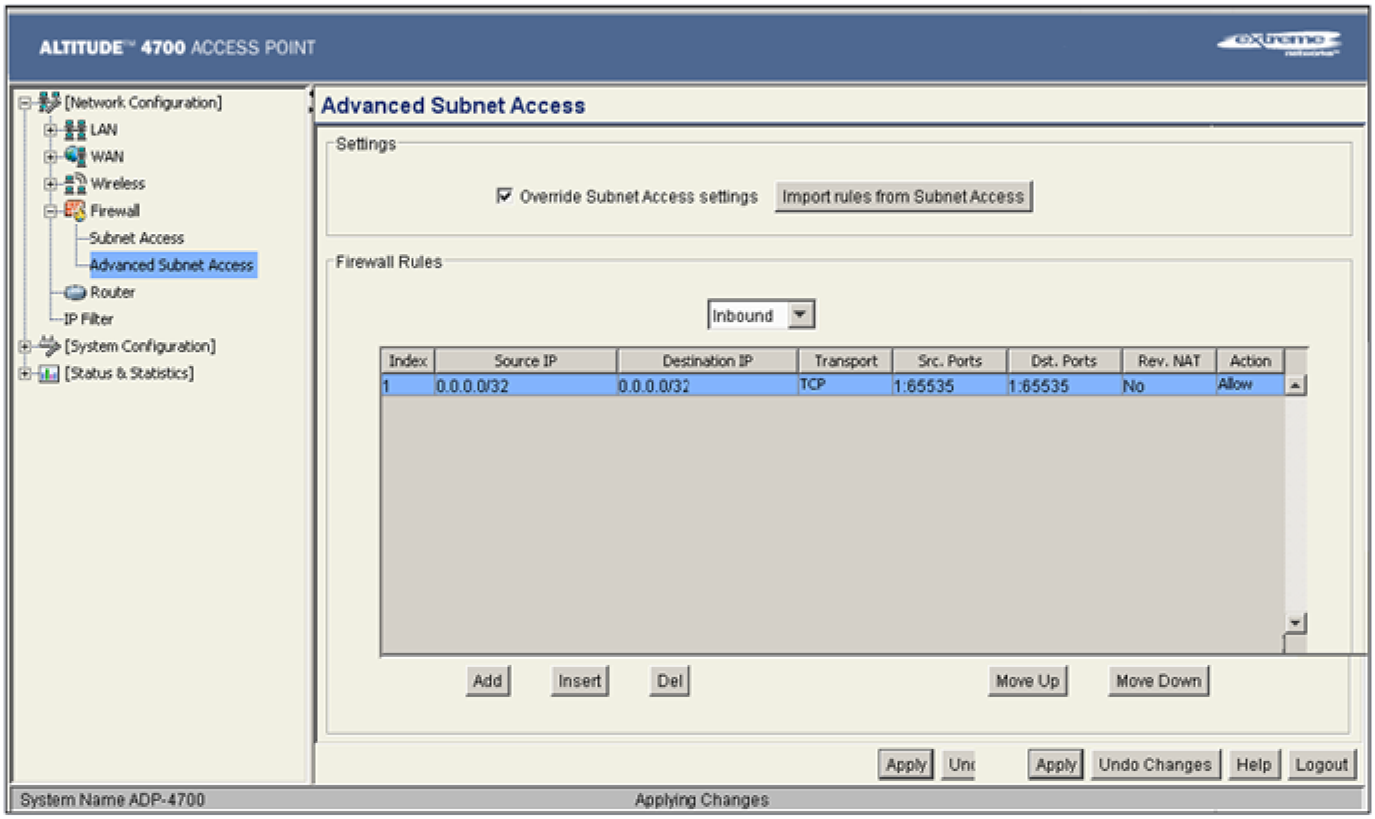
  AH provides authentication, proving the packet sender really is the sender, and the data really is the data sent. AH can be used in transport mode, providing security between two end points. Also, AH can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).
- *ESP*—*Encapsulating Security Protocol* is one of two key components of IPsec. The other key component is *Authentication Header* (AH). ESP encrypts the packets and provides authentication services. ESP can be used in transport mode, providing security between two end points. ESP can also be used in tunnel mode, providing security like that of a *Virtual Private Network (VPN).*
- *GRE*—*General Routing Encapsulation* supports VPNs across the Internet. GRE is a mechanism for encapsulating network layer protocols over any other network layer protocol. Such encapsulation allows routing of IP packets between private IP networks across an Internet using globally assigned IP addresses.

Configuring Advanced Subnet Access

Use the *Advanced Subnet Access* screen to configure complex access rules and filtering based on source port, destination port, and transport protocol. To enable advanced subnet access, the subnet access rules must be overridden. However, the Advanced Subnet Access screen allows you to import existing subnet access rules into the advanced subnet access rules.

To configure access point Advanced Subnet Access:

1 Select *Network Configuration > Firewall > Advanced Subnet Access* from the access point menu tree.



Advanced Subnet Access

Settings

☑ Override Subnet Access settings

Firewall Rules

Inbound

Index	Source IP	Destination IP	Transport	Src. Ports	Dst. Ports	Rev. NAT	Action
1	0.0.0.0/32	0.0.0.0/32	TCP	1:65535	1:65535	No	Allow

System Name ADP-4700

Applying Changes

2 Configure the *Settings* field as needed to override the settings in the Subnet Access screen and import firewall rules into the Advanced Subnet Access screen.

Override Subnet Access settings

Select this checkbox to enable advanced subnet access rules and disable existing subnet access rules, port forwarding, and 1 to many mappings from the system. Only enable advanced subnet access rules if your configuration requires rules that cannot be configured within the *Subnet Access* screen.

Import rules from Subnet Access

Select this checkbox to import existing access rules (NAT, packet forwarding, VPN rules etc.) into the *Firewall Rules* field. This rule import overrides any existing rules configured in the Advanced Subnet Access screen. A warning box displays stating the operation cannot be undone.

3 Configure the *Firewall Rules* field as required add, insert or delete firewall rules into the list of advanced rules.

Inbound or Outbound

Select *Inbound* or *Outbound* from the drop-down menu to specify if a firewall rule is intended for inbound traffic to an interface or outbound traffic from that interface.

Add

Click the *Add* button to insert a new rule at the bottom of the table. Click on a row to display a new window with configuration options for that field.

Insert

Click the *Insert* button to insert a new rule directly above a selected rule in the table. Clicking on a field in the row displays a new window with configuration options.

Del (Delete)

Click *Del* to remove the selected rule from the table. The index numbers for all the rows below the deleted row decrease by 1.

Move Up

Clicking the *Move Up* button moves the selected rule up by one row in the table. The index numbers for the affected rows adjust to reflect the new order.

Move Down

Clicking the *Move Down* button moves the selected rule down by one row in the table. The index numbers for the affected rows adjust to reflect the new order.

Index

The index number determines the order firewall rules are executed. Rules are executed from the lowest number to the highest number.

Source IP

The *Source IP* range defines the origin address or address range for the firewall rule. To configure the Source IP range, click on the field. A new window displays for entering the IP address and range.

Destination IP

The *Destination IP* range determines the target address or address range for the firewall rule. To configure the Destination IP range, click on the field. A new window displays for entering the IP address and range.

Transport

Select a protocol from the drop-down list. For a detailed description of the protocols available, see "Available Protocols" on page 223.

Src. Ports (Source Ports)

The source port range determines which ports the firewall rule applies to on the source IP address. Click on the field to configure the source port range. A new window displays to enter the starting and ending port ranges. For rules where only a single port is necessary, enter the same port in the start and end port fields.

Dst. Ports (Destination Ports

The destination port range determines which ports the firewall rule applies to on the destination IP address. Click on the field to configure the destination port range. A new window displays to enter the starting and ending ports in the range. For rules where only a single port is necessary, enter the same port in the start and end port fields.

4 Click *Apply* to save any changes to the Advanced Subnet Access screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

5 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Advanced Subnet Access screen to the last saved configuration.

6 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring VPN Tunnels

Create a VPN tunnel to ensure data privacy between two end points, even while using an insecure communication medium like the Internet. VPNs use a secure tunnel between two end points as if they are directly connected over a secure connection.

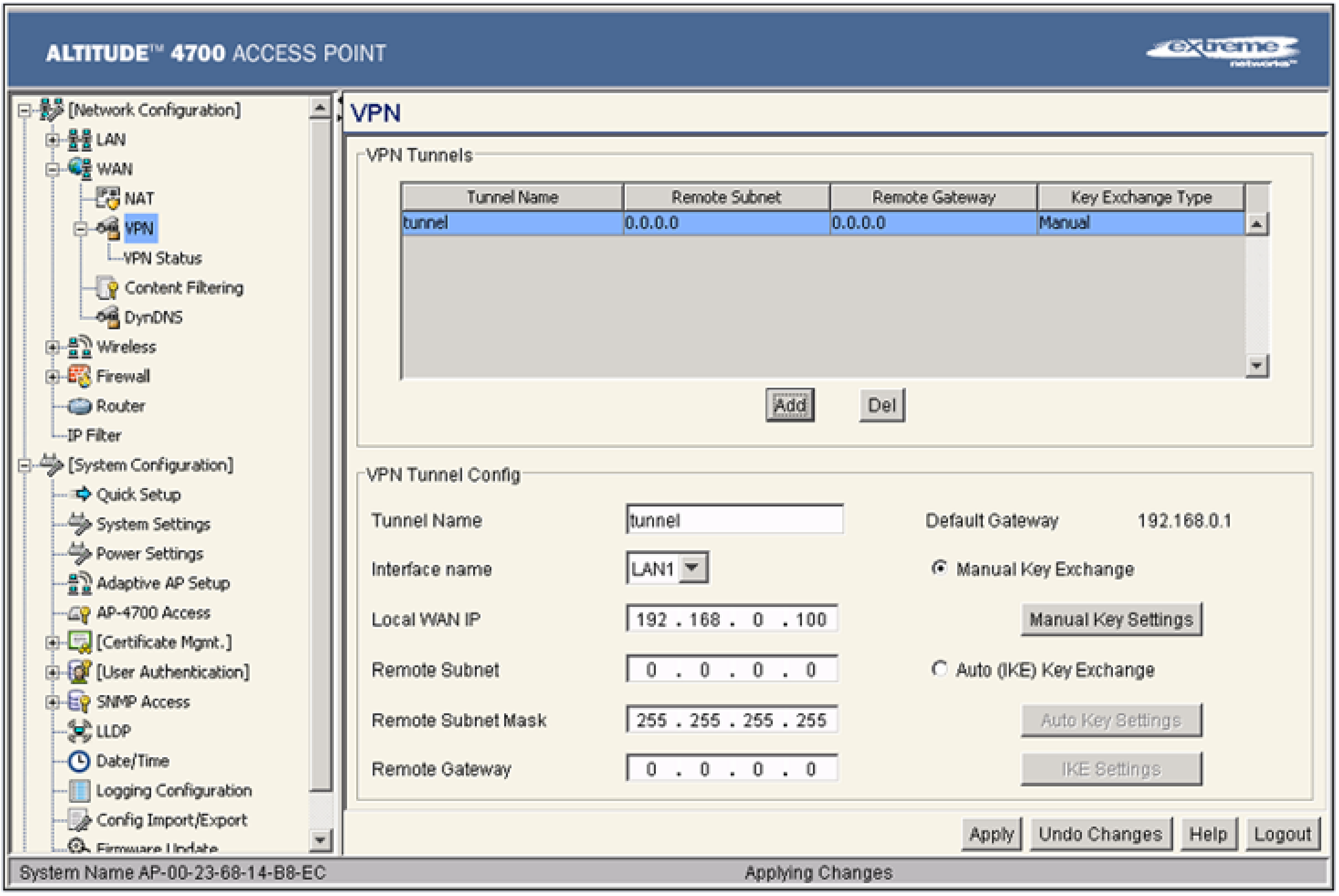
The access point allows up to 25 VPN tunnels to either a VPN endpoint or to another access point. VPN tunnels allow all traffic on a local subnet to route securely through an IPSec tunnel to a private network. A VPN port is a virtual port which handles tunneled traffic. VPN is also supported with the Access Point's new WWAN feature. For more information, see "WAN Failover" on page 19.

When connecting to another site using a VPN, the traffic is encrypted so if anyone intercepts the traffic, they cannot see what it is unless they can break the encryption. The traffic is encrypted from your computer through the network to the VPN. At that point the traffic is decrypted.

Use the *VPN* screen to add and remove VPN tunnels. To configure an existing VPN tunnel, select it from the list in the *VPN Tunnels* field. The selected tunnel's configuration displays in a *VPN Tunnel Config* field.

To configure a VPN tunnel on the access point:

1 Select *Network Configuration* > *WAN* > *VPN* from the access point menu tree.



VPN

VPN Tunnels

Tunnel Name	Remote Subnet	Remote Gateway	Key Exchange Type
tunnel	0.0.0.0	0.0.0.0	Manual

VPN Tunnel Config

Tunnel Name: tunnel

Interface name: LAN1

Local WAN IP: 192 . 168 . 0 . 100

Remote Subnet: 0 . 0 . 0 . 0

Remote Subnet Mask: 255 . 255 . 255 . 255

Remote Gateway: 0 . 0 . 0 . 0

Default Gateway 192.168.0.1

● Manual Key Exchange

○ Auto (IKE) Key Exchange

System Name AP-00-23-68-14-B8-EC

Applying Changes

2 Use the *VPN Tunnels* field to add or delete a tunnel to the list of available tunnels, list tunnel network address information and display key exchange information for each tunnel.

Add	Click *Add* to add a VPN tunnel to the list. To configure a specific tunnel, select it from the list and use the parameters within the *VPN Tunnel Config* field to set its properties.

Del	Click *Del* to delete a highlighted VPN tunnel. There is no confirmation before deleting the tunnel.
Tunnel Name	The *Tunnel Name* column lists the name of each VPN tunnel on the access point.
Remote Subnet	The *Remote Subnet* column lists the remote subnet for each tunnel. The remote subnet is the subnet the remote network uses for connection.
Remote Gateway	The *Remote Gateway* column lists a remote gateway IP address for each tunnel. The numeric remote gateway is the gateway IP address on the remote network the VPN tunnel connects to. Ensure the address is the same as the WAN port address of the target gateway AP or controller.
Key Exchange Type	The *Key Exchange Type* column lists the key exchange type for passing keys between both ends of a VPN tunnel. If *Manual Key Exchange* is selected, this column displays Manual. If *Auto (IKE) Key Exchange* is selected, the field displays *Automatic*.

NOTE

When creating a tunnel, the remote subnet and remote subnet mask must be that of the target device's LAN settings. The remote gateway must be that of the target device's WAN IP address.

If Access Point #1 has the following values:

- *WAN IP address*: 20.1.1.2
- *LAN IP address:* 10.1.1.1
- *Subnet Mask:* 255.0.0.0

Then, the VPN values for Access Point #2 should be:

- Remote subnet: 10.1.1.0 or 10.0.0.0
- Remote subnet mask: 255.0.0.0
- Remote gateway: 20.1.1.2

3 If a VPN tunnel has been added to the list of available access point tunnels, use the *VPN Tunnel Config* field to optionally modify the tunnel's properties.

Tunnel Name	Enter a name to define the VPN tunnel. The tunnel name is used to uniquely identify each tunnel. Select a name best suited to that tunnel's function so it can be selected again in the future if required in a similar application.
Interface name	Use the drop-down menu to specify the LAN1, LAN2 or WAN connection used for routing VPN traffic. Remember, only one LAN connection can be active on the Access Point Ethernet port at a time. The LAN connection specified from the LAN screen to receive priority for Ethernet port connectivity may be the better subnet to select for VPN traffic.
Local WAN IP	Enter the WAN's numerical (non-DNS) IP address in order for the tunnel to pass traffic to a remote network.
Remote Subnet	Specify the numerical (non-DNS) IP address for the Remote Subnet.
Remote Subnet Mask	Enter the subnet mask for the tunnel's remote network for the tunnel. The remote subnet mask is the subnet setting for the remote network the tunnel connects to.

Remote Gateway	Enter a numerical (non-DNS) remote gateway IP address for the tunnel. The remote gateway IP address is the gateway address on the remote network the VPN tunnel connects to.
Default Gateway	Displays the WAN interface's default gateway IP address.
Manual Key Exchange	Selecting *Manual Key Exchange* requires you to manually enter keys for AH and/or ESP encryption and authentication. Click the *Manual Key Settings* button to configure the settings.
Manual Key Settings	Select *Manual Key Exchange* and click the *Manual Key Settings* button to open a screen where AH authentication and ESP encryption/authentication can be configured and keys entered. For more information, see “Configuring Manual Key Settings” on page 230.
Auto (IKE) Key Exchange	Select the Auto (IKE) Key Exchange checkbox to configure AH and/or ESP without having to manually enter keys. The keys automatically generate and rotate for the authentication and encryption type selected.
Auto Key Settings	Select the Auto (IKE) Key Exchange checkbox, and click the *Auto Key Settings* button to open a screen where AH authentication and ESP encryption/authentication can be configured. For more information, see “Configuring Auto Key Settings” on page 233.
IKE Settings	After selecting Auto (IKE) Key Exchange, click the *IKE Settings* button to open a screen where IKE specific settings can be configured. For more information, see “Configuring IKE Key Settings” on page 235.

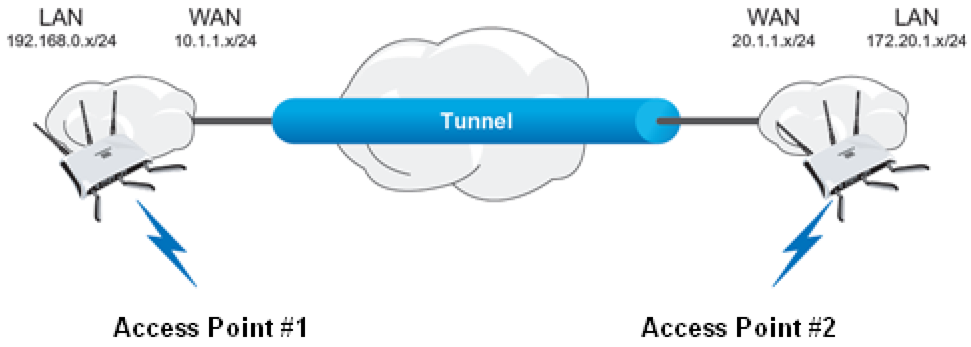
4 Click *Apply* to save any changes to the *VPN* screen as well as changes made to the Auto Key Settings, IKE Settings and Manual Key Settings screens. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.

5 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the VPN, Auto Key Settings, IKE Settings and Manual Key Settings screens to the last saved configuration.

6 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Creating a VPN Tunnel between Two Access Points

This section describes how to define a simple configuration using two Access Points to create an IPSec tunnel.



To create a IPSec VPN tunnel between two Access Points:

1 Ensure the WAN ports are connected via the internet

2 Select *Network Configuration* > *WAN* > *VPN* from the access point menu tree.

3 Enter any tunnel name (tunnel names do not need to match).

4 Enter the WAN port IP address of AP #1 in the *Local WAN IP* field.

5 Enter the LAN IP subnet and mask of AP #2 in the *Remote Subnet* and *Remote Subnet Mask* fields.

6 Enter the WAN port IP address of AP #2 in the *Remote Gateway* field.

7 Click *Add* to add the tunnel to the list.

8 Select the *Auto (IKE) Key Exchange* button.

9 Select *Auto Key Settings*.

10 Select *ESP with Authentication* and *AES 128-bit*. Click *OK*.

11 Select the *IKE Settings* button.

12 Select *Pre Shared Key (PSK)*.

13 Enter the Passphrase.

Passphrases must match on both VPN devices.

14 Select *AES 128-bit*.

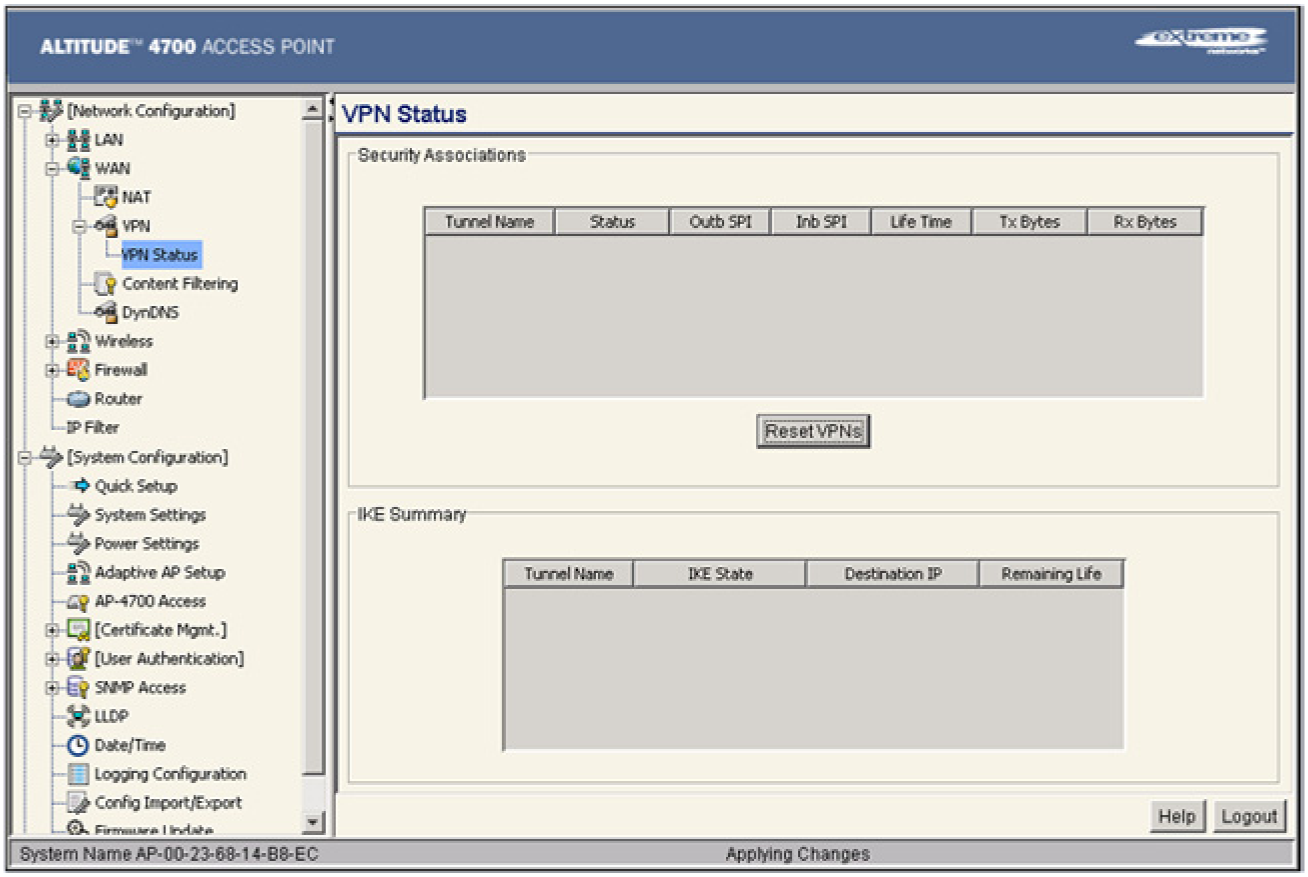
15 Select *Group 2*.

16 Click *OK*.

This will take you back to the main VPN configuration screen.

17 Click *Apply* to save the updates

18 Select *Network Configuration* > *WAN* > *VPN* > *VPN Status* from the access point menu tree. Check the VPN status on the Access Point.



VPN Status

Security Associations

Tunnel Name	Status	Outb SPI	Inb SPI	Life Time	Tx Bytes	Rx Bytes

IKE Summary

Tunnel Name	IKE State	Destination IP	Remaining Life

System Name AP-00-23-68-14-B8-EC

Applying Changes

Notice the status displays “NOT_ACTIVE”. This screen automatically refreshes to get the current status of the VPN tunnel. Once the tunnel is active, the IKE_STATE changes from NOT_CONNECTED to SA_MATURE.

19 On AP #2, repeat the same steps as above. However, replace AP #2 information with AP #1 information.

20 Once both tunnels are established, ping each side to ensure connectivity.

Configuring Manual Key Settings

A transform set is a combination of security protocols and algorithms applied to IPSec protected traffic. During *security association (SA)* negotiation, both gateways agree to use a particular transform set to protect data flow.

A transform set specifies one or two IPSec security protocols (either AH, ESP, or both) and specifies the algorithms to use for the selected security protocol. If you specify an ESP protocol in a transform set, specify just an ESP encryption transform or both an ESP encryption transform and an ESP authentication transform.

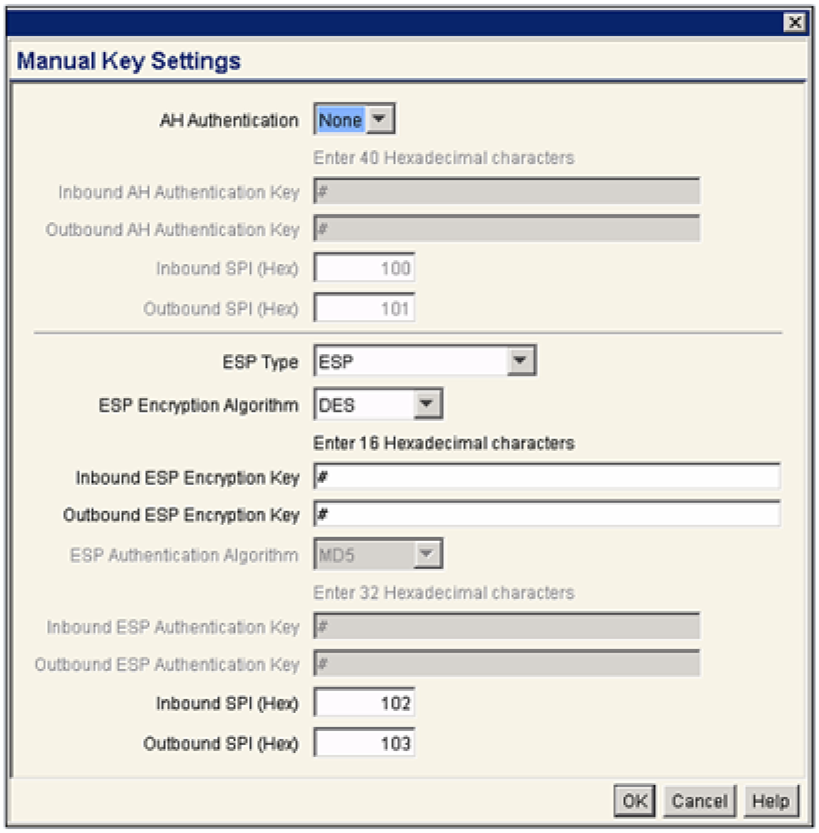
When the particular transform set is used during negotiations for IPSec SAs, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote end of the gateway.

Use the *Manual Key Settings* screen to specify the transform sets used for VPN access.

To configure manual key settings for the access point:

1 Select *Network Configuration* > *WAN* > *VPN* from the access point menu tree.

2 Refer to the *VPN Tunnel Config* field, select the *Manual Key Exchange* radio button and click the *Manual Key Settings* button.



Manual Key Settings

AH Authentication: None

Enter 40 Hexadecimal characters

Inbound AH Authentication Key: #

Outbound AH Authentication Key: #

Inbound SPI (Hex): 100

Outbound SPI (Hex): 101

ESP Type: ESP

ESP Encryption Algorithm: DES

Enter 16 Hexadecimal characters

Inbound ESP Encryption Key: #

Outbound ESP Encryption Key: #

ESP Authentication Algorithm: MD5

Enter 32 Hexadecimal characters

Inbound ESP Authentication Key: #

Outbound ESP Authentication Key: #

Inbound SPI (Hex): 102

Outbound SPI (Hex): 103

3 Configure the *Manual Key Settings* screen to modify the following:

NOTE

When entering Inbound or Outbound encryption or authentication keys, an error message could display stating the keys provided are “weak”. Some WEP attack tools invoke a dictionary to hack WEP keys based on commonly used words. To avoid entering a weak key, try to not to produce a WEP key using commonly used terms and attempt to mix alphabetic and numerical key attributes when possible.

AH Authentication

AH provides data authentication and anti-replay services for the VPN tunnel. Select the required authentication method from the drop-down menu:

- *None*—Disables AH authentication. The rest of the fields are not active.
- *MD5*—Enables the Message Digest 5 algorithm requiring 128-bit (32-character hexadecimal) keys.
- *SHA1*—Enables Secure Hash Algorithm 1, requiring 160-bit (40-character hexadecimal) keys.

Inbound AH Authentication Key

Configure a key for computing the integrity check on inbound traffic with the selected authentication algorithm. The key must be 32/40 (for MD5/SHA1) hexadecimal (0-9, A-F) characters in length. The key value must match the corresponding outbound key on the remote security gateway.

Outbound AH Authentication Key

Configure a key for computing the integrity check on outbound traffic with the selected authentication algorithm. The key must be 32/40 (for MD5/SHA1) hexadecimal (0-9, A-F) characters in length. The key value must match the corresponding inbound key on the remote security gateway.

Inbound SPI (Hex)

Enter an up to six-character hexadecimal value to identify the inbound security association created by the AH algorithm. The value must match the corresponding outbound SPI value configured on the remote security gateway.

Outbound SPI (Hex)

Provide an up to six-character hexadecimal value to identify the outbound security association created by the AH algorithm. The value must match the corresponding inbound SPI value configured on the remote security gateway.

ESP Type

ESP provides packet encryption, optional data authentication and anti-replay services for the VPN tunnel. Use the drop-down menu to select the ESP type. Options include:

- *None*—Disables ESP. The rest of the fields are not be active.
- *ESP*—Enables ESP for the tunnel.
- *ESP with Authentication*—Enables ESP with authentication.

ESP Encryption Algorithm

Select the encryption and authentication algorithms for the VPN tunnel using the drop-down menu.

- *DES*—Uses the DES encryption algorithm requiring 64-bit (16-character hexadecimal) keys.
- *3DES*—Uses the 3DES encryption algorithm requiring 192-bit (48-character hexadecimal) keys.
- *AES 128-bit*—Uses the Advanced Encryption Standard algorithm with 128-bit (32-character hexadecimal) keys.
- *AES 192-bit*—Uses the Advanced Encryption Standard algorithm with 192-bit (48-character hexadecimal) keys.
- *AES 256-bit*—Uses the Advanced Encryption Standard algorithm with 256-bit (64-character hexadecimal) keys.

Inbound ESP Encryption Key

Enter a key for inbound traffic. The length of the key is determined by the selected encryption algorithm. The key must match the outbound key at the remote gateway.

Outbound ESP Encryption Key

Define a key for outbound traffic. The length of the key is determined by the selected encryption algorithm. The key must match the inbound key at the remote gateway.

ESP Authentication Algorithm	Select the authentication algorithm to use with ESP. This option is available only when *ESP with Authentication* was selected for the ESP type. Options include: • *MD5*—Enables the Message Digest 5 algorithm, which requires 128-bit (32-character hexadecimal) keys. • *SHA1*—Enables Secure Hash Algorithm 1, which requires 160-bit (40-character hexadecimal) keys.
Inbound ESP Authentication Key	Define a key for computing the integrity check on the inbound traffic with the selected authentication algorithm. The key must be 32/40 (for MD5/SHA1) hexadecimal (0-9, A-F) characters in length. The key must match the corresponding outbound key on the remote security gateway.
Outbound ESP Authentication Key	Enter a key for computing the integrity check on outbound traffic with the selected authentication algorithm. The key must be 32/40 (for MD5/SHA1) hexadecimal (0-9, A-F) characters in length. The key must match the corresponding inbound key on the remote security gateway.
Inbound SPI (Hex)	Define an (up to) six-character (maximum) hexadecimal value to identify the inbound security association created by the encryption algorithm. The value must match the corresponding outbound SPI value configured on the remote security gateway.
Outbound SPI (Hex)	Enter an (up to) six-character (maximum) hexadecimal value to identify the outbound security association created by the encryption algorithm. The value must match the corresponding inbound SPI value configured on the remote security gateway.

The Inbound and Outbound SPI settings are required to be interpolated to function correctly. For example:

- *AP1 Inbound SPI* = 800
- *AP1 Outbound SPI* = 801
- *AP2 Inbound SPI* = 801
- *AP2 Outbound SPI* = 800

4 Click *Ok* to return to the VPN screen. Click *Apply* to retain the settings made on the *Manual Key Settings* screen.

5 Click *Cancel* to return to the VPN screen without retaining the changes made to the *Manual Key Settings* screen.

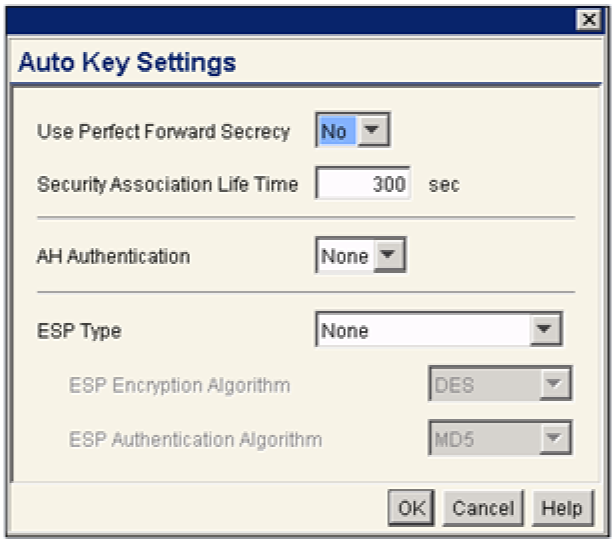
Configuring Auto Key Settings

The access point's Network Management System can automatically set encryption and authentication keys for VPN access. Use the *Auto Key Settings* screen to specify the type of encryption and authentication, without specifying the keys. To manually specify keys, cancel out of the *Auto Key Settings* screen, select the *Manual Key Exchange* radio button, and set the keys within the *Manual Key Setting* screen.

To configure auto key settings for the access point:

1 Select *Network Configuration* > *WAN* > *VPN* from the access point menu tree.

2 Refer to the *VPN Tunnel Config* field, select the *Auto (IKE) Key Exchange* radio button and click the *Auto Key Settings* button.



Auto Key Settings

Use Perfect Forward Secrecy: No

Security Association Life Time: 300 sec

AH Authentication: None

ESP Type: None

ESP Encryption Algorithm: DES

ESP Authentication Algorithm: MD5

3 Configure the *Auto Key Settings* screen to modify the following:

Use Perfect Forward Secrecy
: Forward secrecy is a key-establishment protocol guaranteeing the discovery of a session key or long-term private key does not compromise the keys of other sessions. Select *Yes* to enable Perfect Forward Secrecy. Select *No* to disable Perfect Forward Secrecy.

Security Association Life Time
: The Security Association Life Time is the configurable interval used to timeout association requests that exceed the defined interval. The available range is from 300 to 65535 seconds. The default is 300 seconds.

AH Authentication
: AH provides data authentication and anti-replay services for the VPN tunnel. Select the desired authentication method from the drop-down menu.

- *None*—Disables AH authentication. No keys are required to be manually provided.
- *MD5*—Enables the Message Digest 5 algorithm. No keys are required to be manually provided.
- *SHA1*—Enables Secure Hash Algorithm 1. No keys are required to be manually provided.

ESP Type
: ESP provides packet encryption, optional data authentication and anti-replay services for the VPN tunnel. Use the drop-down menu to select the ESP type.

- *None*—Disables ESP. The rest of the fields are not active.
- *ESP*—Enables ESP for this tunnel.
- *ESP with Authentication*—Enables ESP with authentication.

ESP Encryption Algorithm

Use this menu to select the encryption and authentication algorithms for this VPN tunnel.

- *DES*—Selects the DES algorithm.No keys are required to be manually provided.
- *3DES*—Selects the 3DES algorithm. No keys are required to be manually provided.
- *AES 128-bit*—Selects the Advanced Encryption Standard algorithm with 128-bit. No keys are required to be manually provided.
- *AES 192-bit*—Selects the Advanced Encryption Standard algorithm with 192-bit. No keys are required to be manually provided.
- *AES 256-bit*—Selects the Advanced Encryption Standard algorithm with 256-bit. No keys are required to be manually provided.

ESP Authentication Algorithm

Use this menu to select the authentication algorithm to be used with ESP. This menu is only active when ESP with Authentication was selected for the ESP type.

- *MD5*—Enables the Message Digest 5 algorithm requiring 128-bit. No keys are required to be manually provided.
- *SHA1*—Enables Secure Hash Algorithm. No keys are required to be manually provided.

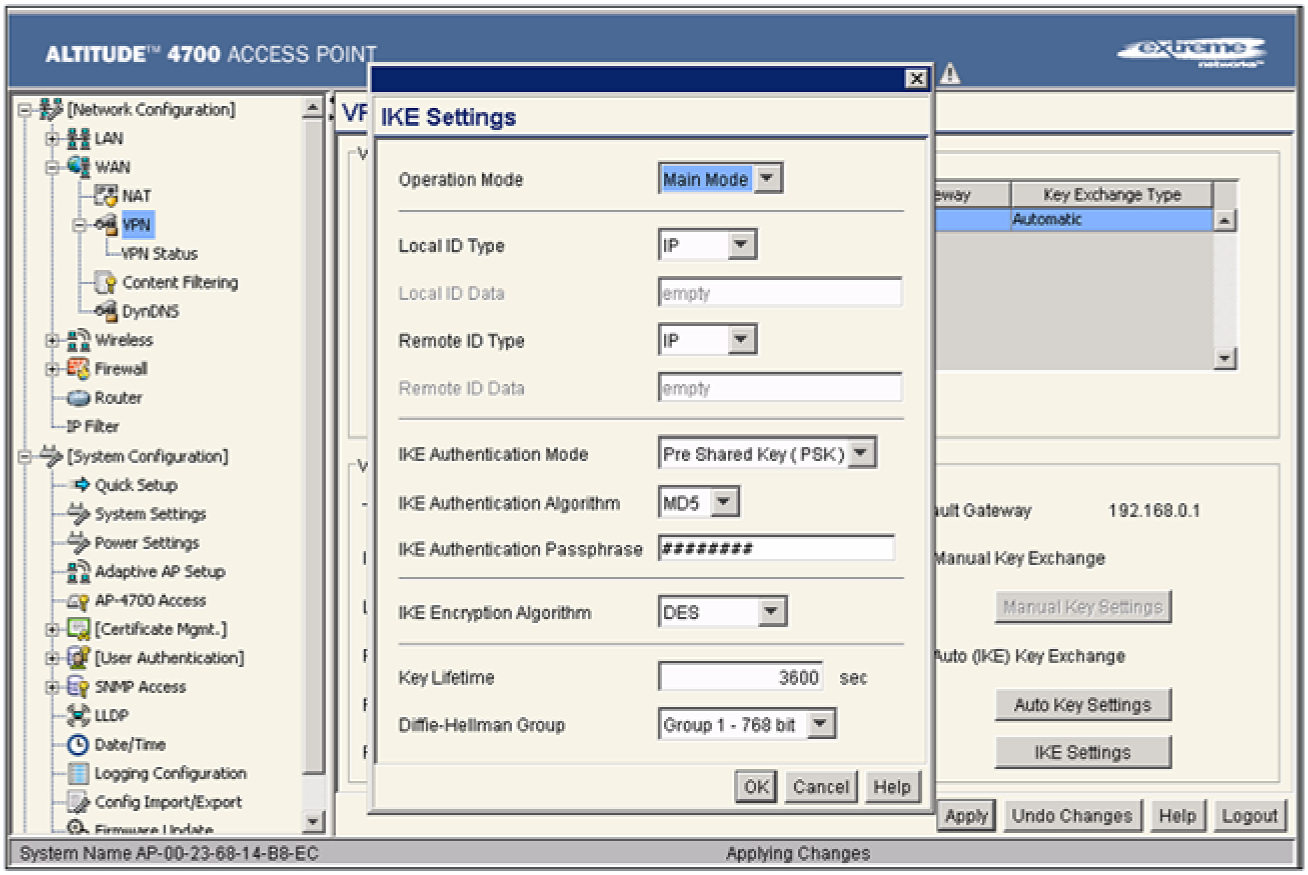
4. Click *Ok* to return to the VPN screen. Click Apply to retain the settings made on the *Auto Key Settings* screen.
5. Click *Cancel* to return to the VPN screen without retaining the changes made to this screen.

Configuring IKE Key Settings

The *Internet Key Exchange (IKE)* is an IPsec standard protocol used to ensure security for VPN negotiation and remote host or network access. IKE provides an automatic means of negotiation and authentication for communication between two or more parties. In essence, IKE manages IPSec keys automatically for the parties.

To configure IKE key settings for the access point:

1. Select *Network Configuration* > *WAN* > *VPN* from the access point menu tree.
2. Refer to the *VPN Tunnel Config* field, select the *Auto (IKE) Key Exchange* radio button and click the *IKE Settings* button.



IKE Settings

Operation Mode: Main Mode

Local ID Type: IP

Local ID Data: empty

Remote ID Type: IP

Remote ID Data: empty

IKE Authentication Mode: Pre Shared Key (PSK)

IKE Authentication Algorithm: MD5

IKE Authentication Passphrase: ########

IKE Encryption Algorithm: DES

Key Lifetime: 3600 sec

Diffie-Hellman Group: Group 1 - 768 bit

Key Exchange Type: Automatic

Default Gateway: 192.168.0.1

Manual Key Exchange

Auto (IKE) Key Exchange

System Name AP-00-23-68-14-B8-EC

Applying Changes

3 Configure the *IKE Key Settings* screen to modify the following:

Operation Mode
: The Phase I protocols of IKE are based on the ISAKMP identity-protection and aggressive exchanges. IKE main mode refers to the identity-protection exchange, and IKE aggressive mode refers to the aggressive exchange.

- *Main*—Standard IKE mode for communication and key exchange.
- *Aggressive*—Aggressive mode is faster, but less secure than Main mode. Identities are not encrypted unless public key encryption is used. The authentication method cannot be negotiated if the initiator chooses public key encryption

Local ID Type
: Select the type of ID to be used for the access point end of the SA.

- *IP*—Select IP if the local ID type is the IP address specified as part of the tunnel.
- *FQDN*—Use FQDN if the local ID is a fully qualified domain name (such as extremenetworks.com).
- *UFQDN*—Select UFQDN if the local ID is a user fully-qualified email (such as johndoe@extremenetworks.com).

Local ID Data
: Specify the FQDN or UFQDN based on the Local ID type assigned.

Remote ID Type

Select the type of ID to be used for the access point end of the tunnel from the *Remote ID Type* drop-down menu.

- *IP*—Select the IP option if the remote ID type is the IP address specified as part of the tunnel.
- *FQDN*—Select FQDN if the remote ID type is a fully qualified domain name (such as extremenetworks.com). The setting for this field does not have to be fully qualified, however it must match the setting for the Certificate Authority.
- *UFQDN*—Select this item if the remote ID type is a user unqualified email address (such as johndoe@extremenetworks.com). The setting for this field does not have to be unqualified, it just must match the setting of the field of the Certificate Authority.

Remote ID Data

If FQDN or UFQDN is selected, specify the data (either the qualified domain name or the user name) in the *Remote ID Data* field.

IKE Authentication Mode

Select the appropriate IKE authentication mode:

- *Pre-Shared Key (PSK)*—Specify an authenticating algorithm and passcode used during authentication.
- *RSA Certificates*—Select this option to use RSA certificates for authentication purposes. See the CA Certificates and Self certificates screens to create and import certificates into the system.

IKE Authentication Algorithm

IKE provides data authentication and anti-replay services for the VPN tunnel. Select an authentication methods from the drop-down menu.

- *MD5*—Enables the Message Digest 5 algorithm. No keys are required to be manually provided.
- *SHA1*—Enables Secure Hash Algorithm. No keys are required to be manually provided.

IKE Authentication Passphrase

If you selected *Pre-Shared Key* as the authentication mode, you must provide a passphrase.

IKE Encryption Algorithm

Select the encryption and authentication algorithms for the VPN tunnel from the drop-down menu.

- *DES*—Uses the DES encryption algorithm. No keys are required to be manually provided.
- *3DES*—Enables the 3DES encryption algorithm. No keys are required to be manually provided.
- *AES 128-bit*—Uses the Advanced Encryption Standard algorithm with 128-bit. No keys are required to be manually provided.
- *AES 192-bit*—Enables the Advanced Encryption Standard algorithm with 192-bit. No keys are required to be manually provided.
- *AES 256-bit*—Uses the Advanced Encryption Standard algorithm with 256-bit. No keys are required to be manually provided.

Key Lifetime

The number of seconds the key is valid. At the end of the lifetime, the key is renegotiated.

The access point forces renegotiation every 3600 seconds. There is no way to change the renegotiation value. If the IKE Lifetime is greater than 3600, the keys still get renegotiated every 3600 seconds.

Diffie Hellman Group

Select a *Diffie-Hellman Group* to use. The Diffie-Hellman key agreement protocol allows two users to exchange a secret key over an insecure medium without any prior secrets. Two algorithms exist, 768-bit and 1024-bit. Select one of the following options:

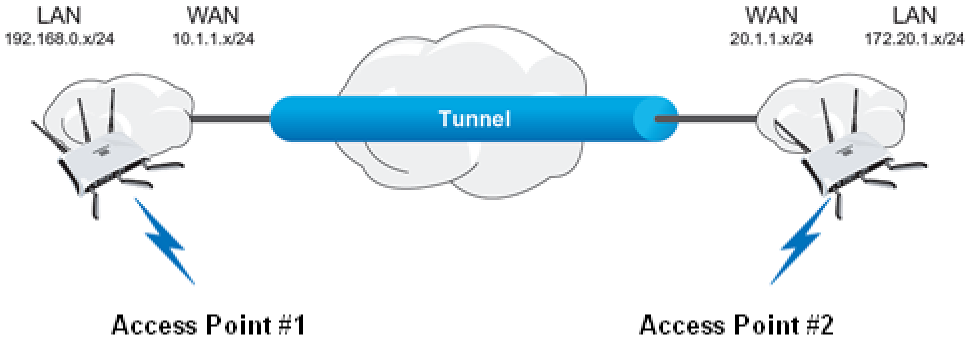
- *Group 1 - 768 bit*—Somewhat faster than the 1024-bit algorithm, but secure enough in most situations.
- *Group 2 - 1024 bit*—Somewhat slower than the 768-bit algorithm, but much more secure and a better choice for extremely sensitive situations.

4 Click *Ok* to return to the VPN screen. Click Apply to retain the settings made on the *IKE Settings* screen.

5 Click *Cancel* to return to the VPN screen without retaining the changes made to the *IKE Settings* screen.

VPN Configuration - Example

The VPN topology used in this example is as follows:



To set the configuration on the Access Points:

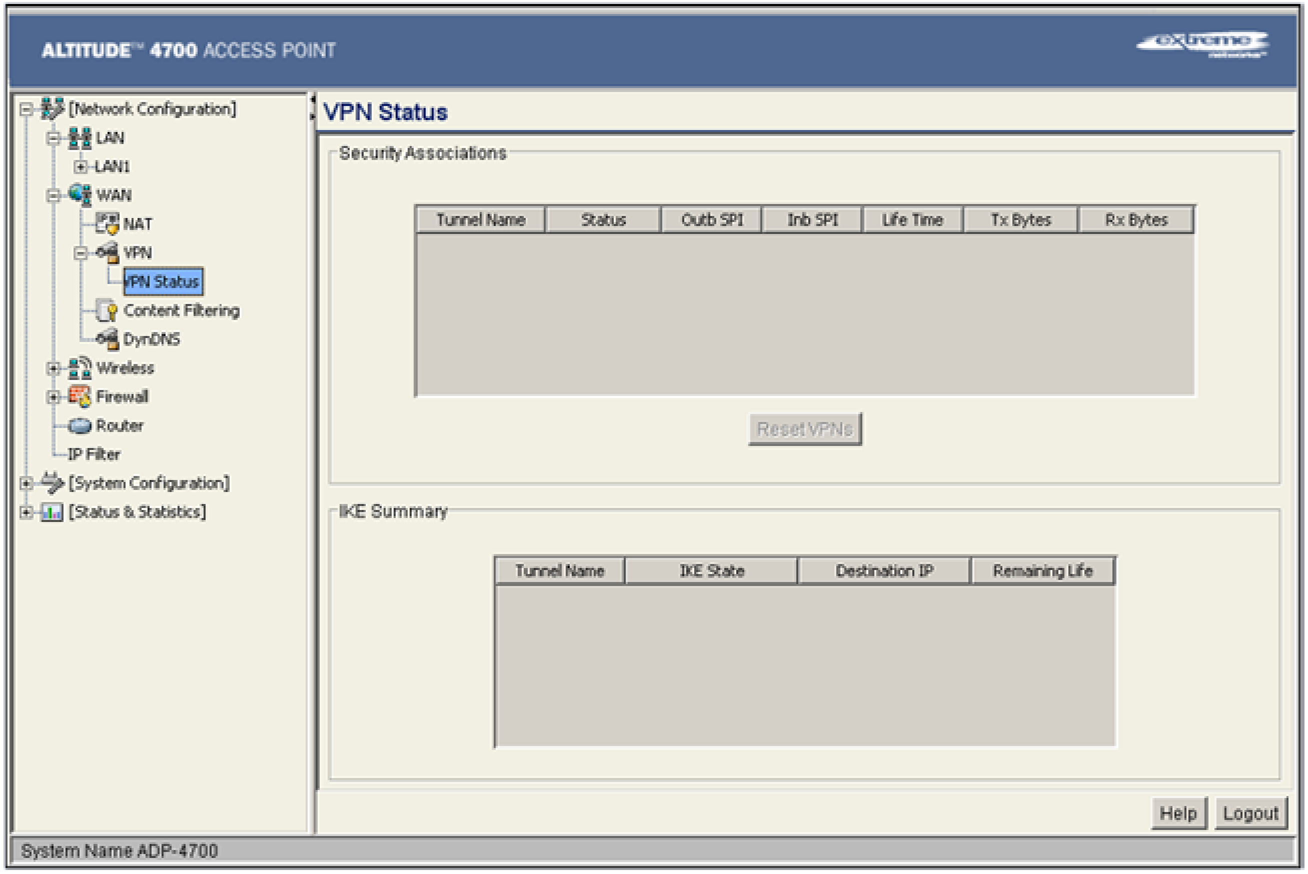
1 Configure the LAN1 interface by statically assigning an IP address of 10.1.1.1.

Viewing VPN Status

Use the *VPN Status* screen to display the status of the tunnels configured on the access point as well as their lifetime, transmit and receive statistics. The VPN Status screen is read-only with no configurable parameters. To configure a VPN tunnel, use the *VPN* configuration screen in the WAN section of the access point menu tree.

To view VPN status:

1 Select *Network Configuration* > *WAN* > *VPN* > *VPN Status* from the access point menu tree.



2 Reference the *Security Associations* field to view the following:

Tunnel Name
The *Tunnel Name* column lists the names of all the tunnels *configured* on the access point. For information on configuring a tunnel, see "Configuring VPN Tunnels" on page 225.

Status
The *Status* column lists the status of each configured tunnel. When the tunnel is not in use, the status reads *NOT_ACTIVE*. When the tunnel is connected, the status reads *ACTIVE*.

Outb SPI
The *Outb SPI* column displays the outbound *Security Parameter Index* (SPI) for each tunnel. The SPI is used locally by the access point to identify a security association. There are unique outbound and inbound SPIs.

Inb SPI
The *Inb SPI* column displays the inbound *Security Parameter Index* (SPI) for each of the tunnels. The SPI is used locally by the access point to identify a security association. There are unique outbound and inbound SPIs.

Life Time
Use the *Life Time* column to view the lifetime associated with a particular Security Association (SA). Each SA has a finite lifetime defined. When the lifetime expires, the SA can no longer be used to protect data traffic. The maximum SA lifetime is 65535 seconds.

Tx Bytes — The *Tx Bytes* column lists the amount of data (in bytes) transmitted through each configured tunnel.

Rx Bytes — The *Rx Bytes* column lists the amount of data (in bytes) received through each configured tunnel.

3 Click the *Reset VPNs* button to reset active VPNs. Selecting *Reset VPNs* forces renegotiation of all the Security Associations and keys. Users could notice a slight pause in network performance.

4 Reference the *IKE Summary* field to view the following:

Tunnel Name — Displays the name of each of the tunnels configured to use IKE for automatic key exchange.

IKE State — Lists the state for each of the tunnels configured to use IKE for automatic key exchange. When the tunnel is not active, the *IKE State* field displays *NOT_CONNECTED.* When the tunnel is active, the *IKE State* field displays *CONNECTED.*

Destination IP — Displays the destination IP address for each tunnel configured to use IKE for automatic key exchange.

Remaining Life — Lists the remaining life of the current IKE key for each tunnel. When the remaining life on the IKE key reaches 0, IKE initiates a negotiation for a new key. IKE keys associated with a renegotiated tunnel.

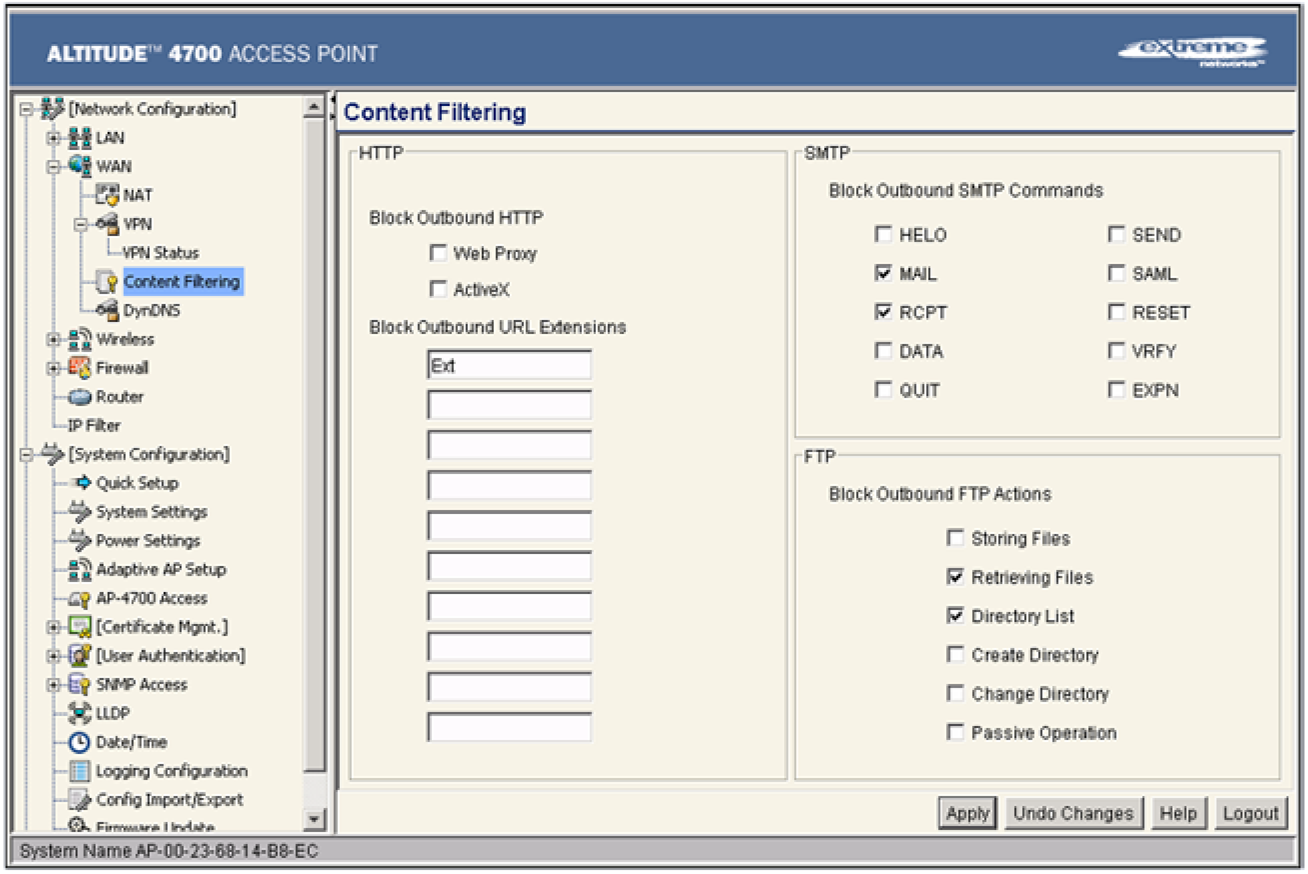
5 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring Content Filtering Settings

Content filtering allows system administrators to block specific commands and URL extensions from going out through the Access Point’s WAN port. Therefore, content filtering affords system administrators selective control on the content proliferating the network and is a powerful data and network screening tool. Content filtering allows the blocking of up to 10 files or URL extensions and allows blocking of specific outbound HTTP, SMTP, and FTP requests.

To configure content filtering for the access point:

1 Select *Network Configuration* > *WAN* > *Content Filtering* from the access point menu tree.



Content Filtering

HTTP

Block Outbound HTTP

□ Web Proxy

□ ActiveX

Block Outbound URL Extensions

Ext

SMTP

Block Outbound SMTP Commands

□ HELO	□ SEND
☑ MAIL	□ SAML
☑ RCPT	□ RESET
□ DATA	□ VRFY
□ QUIT	□ EXPN

FTP

Block Outbound FTP Actions

□ Storing Files

☑ Retrieving Files

☑ Directory List

□ Create Directory

□ Change Directory

□ Passive Operation

System Name AP-00-23-68-14-B8-EC

2 Configure the *HTTP* field to configure block Web proxies and URL extensions.

Block Outbound HTTP

HyperText Transport Protocol (HTTP) is the protocol used to transfer information to and from Web sites. HTTP Blocking allows for blocking of specific HTTP commands going outbound on the access point WAN port. HTTP blocks commands on port 80 only.

The Block Outbound HTTP option allows blocking of the following (user selectable) outgoing HTTP requests:

- *Web Proxy*—Blocks the use of Web proxies by clients
- *ActiveX*—Blocks all outgoing ActiveX requests by clients. Selecting ActiveX only blocks traffic (scripting language) with an .ocx extension.

Block Outbound URL Extensions

Enter a URL extension or file name per line in the format of *filename.ext*. An asterisk (*) can be used as a wildcard in place of the filename to block all files with a specific extension.

3 Configure the *SMTP* field to disable or restrict specific kinds of network mail traffic.

Block Outbound SMTP Commands

Simple Mail Transport Protocol (SMTP) is the Internet standard for host-to-host mail transport. SMTP generally operates over TCP on port 25. SMTP filtering allows the blocking of any or all outgoing SMTP commands. Check the box next to the command to disable that command when using SMTP across the access point's WAN port.

- *HELO*—(Hello) Identifies the SMTP sender to the SMTP receiver.
- *MAIL*—Initiates a mail transaction where data is delivered to one or more mailboxes on the local server.
- *RCPT*—(Recipient) Identifies a recipient of mail data.
- *DATA*—Tells the SMTP receiver to treat the following information as mail data from the sender.
- *QUIT*—Tells the receiver to respond with an *OK* reply and terminate communication with the sender.
- *SEND*—Initiates a mail transaction where mail is sent to one or more remote terminals.
- *SAML*—(Send and Mail) Initiates a transaction where mail data is sent to one or more local mailboxes and remote terminals.
- *RESET*—Cancels mail transaction and informs the recipient to discard data sent during transaction.
- *VRFY*—Asks receiver to confirm the specified argument identifies a user. If argument does identify a user, the full name and qualified mailbox is returned.
- *EXPN*—(Expand) Asks receiver to confirm a specified argument identifies a mailing list. If the argument identifies a list, the membership list of the mailing list is returned.

4 Configure the *FTP* field to block or restrict various FTP traffic on the network.

Block Outbound FTP Actions

File Transfer Protocol (FTP) is the Internet standard for host-to-host mail transport. FTP generally operates over TCP port 20 and 21. FTP filtering allows the blocking of any or all outgoing FTP functions.

Check the box next to the command to disable the command when using FTP across the access point's WAN port.

- *Storing Files*—Blocks the request to transfer files sent from the client across the AP's WAN port to the FTP server.
- *Retrieving Files*—Blocks the request to retrieve files sent from the FTP server across the AP's WAN port to the client.
- *Directory List*—Blocks requests to retrieve a directory listing sent from the client across the AP's WAN port to the FTP server.
- *Create Directory*—Blocks requests to create directories sent from the client across the AP's WAN port to the FTP server.
- *Change Directory*—Blocks requests to change directories sent from the client across the AP's WAN port to the FTP server.
- *Passive Operation*—Blocks passive mode FTP requests sent from the client across the AP's WAN port to the FTP server.

5 Click *Apply* to save any changes to the Content Filtering screen. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.

6 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Content Filtering screen to the last saved configuration.

7 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring Rogue AP Detection

It is possible that not all of the devices identified by the access point are operating legitimately within the access point's radio coverage area. A rogue AP is a device located nearby an authorized Extreme Networks access point but recognized as having properties rendering its operation illegal and threatening to the access point and the LAN. Rogue AP detection can be configured independently for both access point 802.11a/n and 802.11b/g/n radios (if using a dual radio sku access point). A rogue detection interval is the user-defined interval the access point waits to search for rogue APs. Additionally, the Access Point does not detect rogue APs on illegal channels (channels not allowed by the regulatory requirements of the country the Access Point is operating in).

The rogue detection interval is used in conjunction with Motorola MUs that identify themselves as rogue detection capable to the Access Point. The detection interval defines how often the Access Point requests these MUs to scan for a rogue AP. A shorter interval can affect the performance of the MU, but it will also decrease the time it takes for the Access Point to scan for a rogue AP. A longer interval will have less of an impact to the MU's, but it will increase the amount of time used to detect rogue APs.

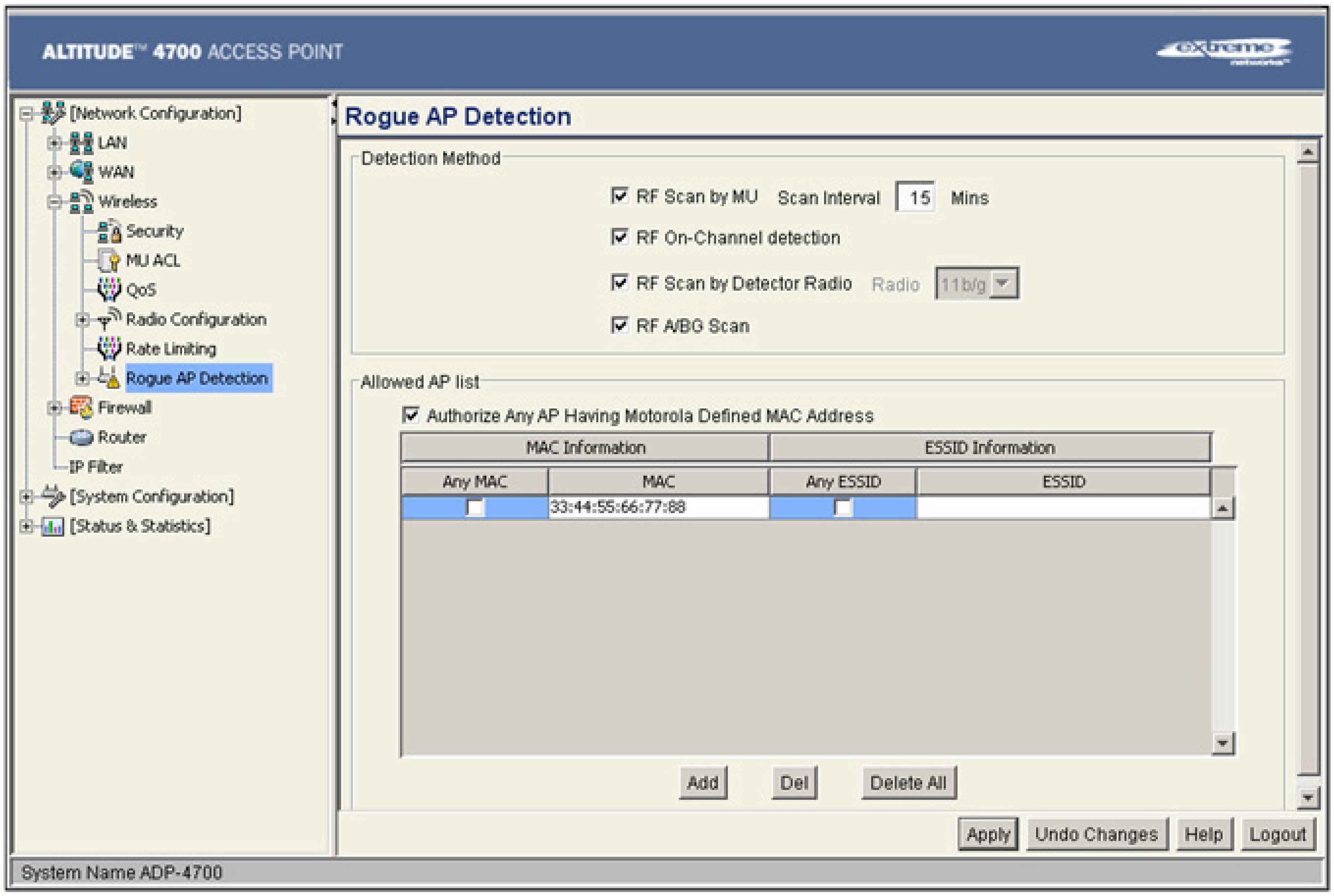
Therefore, the interval should be set according to the perceived risk of rogue devices and the criticality of MU performance.

CAUTION

Using an antenna other than the Dual-Band Antenna could render the access point's Rogue AP Detector Mode feature inoperable. Contact your Extreme Networks sales associate for specific information.

To configure Rogue AP detection for the access point:

1 Select *Network Configuration* > *Wireless* > *Rogue AP Detection* from the access point menu tree.



Rogue AP Detection

Detection Method

☑ RF Scan by MU Scan Interval 15 Mins

☑ RF On-Channel detection

☑ RF Scan by Detector Radio Radio 11b/g

☑ RF A/BG Scan

Allowed AP list

☑ Authorize Any AP Having Motorola Defined MAC Address

MAC Information		ESSID Information	
Any MAC	MAC	Any ESSID	ESSID
□	33:44:55:66:77:88	□	

CAUTION

Users cannot define a rogue detection method when one of the Access Point radios is functioning as a WIPS sensor. To use one of the radios as a detector, you must disable WIPS sensor mode first, then set a radio for the desired detection method.

2 Configure the *Detection Method* field to set the detection method (MU or access point) and define the 802.11a/n or 802.11b/g/n radio to conduct the rogue AP search.

RF Scan by MU

Select the *RF Scan by MU* checkbox to enable MUs to scan for potential rogue APs within the network. Define an interval in the *Scan Interval* field for associated MUs to beacon in an attempt to locate a rogue AP. Set the interval to a value sooner than the default if a large volume of device network traffic is anticipated within the coverage area of the target access point. The *Scan Interval* field is not available unless the RF Scan by MU checkbox is selected. Motorola clients must be associated and have rogue AP detection enabled.

RF On-Channel Detection

Select the *RF On-Channel Detection* checkbox to enable the Access Point to detect rogue APs on its current (legal) channel setting.

RF Scan by Detector Radio

If the Access Point is a dual-radio model, select the *RF Scan by Detector Radio* checkbox to enable the selected 11a or 11b/g radio to scan for rogue APs. For example, if *11b/g* is selected, the existing 11a radio would act as the "detector radio," scanning on all 11b/g channels while the existing 11b/g radio continues to service MUs. The assumption is, when planning to do an all channel scan on one band, the MUs would also be on that band. The radio on the other band is used as the "detector radio."

RF A/BG Scan

Select this checkbox to scan for rouges over all channels on both of the Access Point's 11a and 11bg radio bands. The switching of radio bands is based on a timer with no user intervention required. This option provides a good opportunity to detect rogues, as rogues often roam from one association to a stronger one regardless of the current operating channel.

3 Use the *Allowed AP List* field to restrict Extreme Networks APs from Rogue AP detection and create a list of device MAC addresses and ESSIDs approved for interoperability with the access point.

Authorize Any AP Having Extreme Networks Defined MAC Address

Select this checkbox to enable all Access Points with a Extreme Networks MAC address to interoperate with the access point conducting a scan for rogue devices.

Add

Click *Add* to display a single set of editable MAC address and ESS address values.

Del (Delete)

Click the *Delete* button to remove the highlighted line from the Rule Management field. The MAC and ESS address information previously defined is no longer applicable unless the previous configuration is restored.

Delete All

Click the *Delete All* button to remove all entries from the Rule Management field. All MAC and ESS address information previously defined is no longer applicable unless the previous configuration is restored.

Any MAC

Select the *Any MAC* checkbox to prevent a device's MAC address (whether it is a known device MAC address or not) from being considered a rogue device.

MAC Address

Click *Add,* and enter the device MAC address to be excluded from classification as a rogue device.

Any ESSID

Select the *Any ESSID* checkbox to prevent a device's ESSID (whether it is a known device ESSID or not) from being considered a rogue device

ESSID

Click *Add*, and enter the name of a device ESSID to be excluded from classification as a rogue device. Do not use < > | " & \ ? as characters for the ESSID name.

4 Click *Apply* to save any changes to the Rogue AP Detection screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

5 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Rogue AP Detection screen to the last saved configuration.

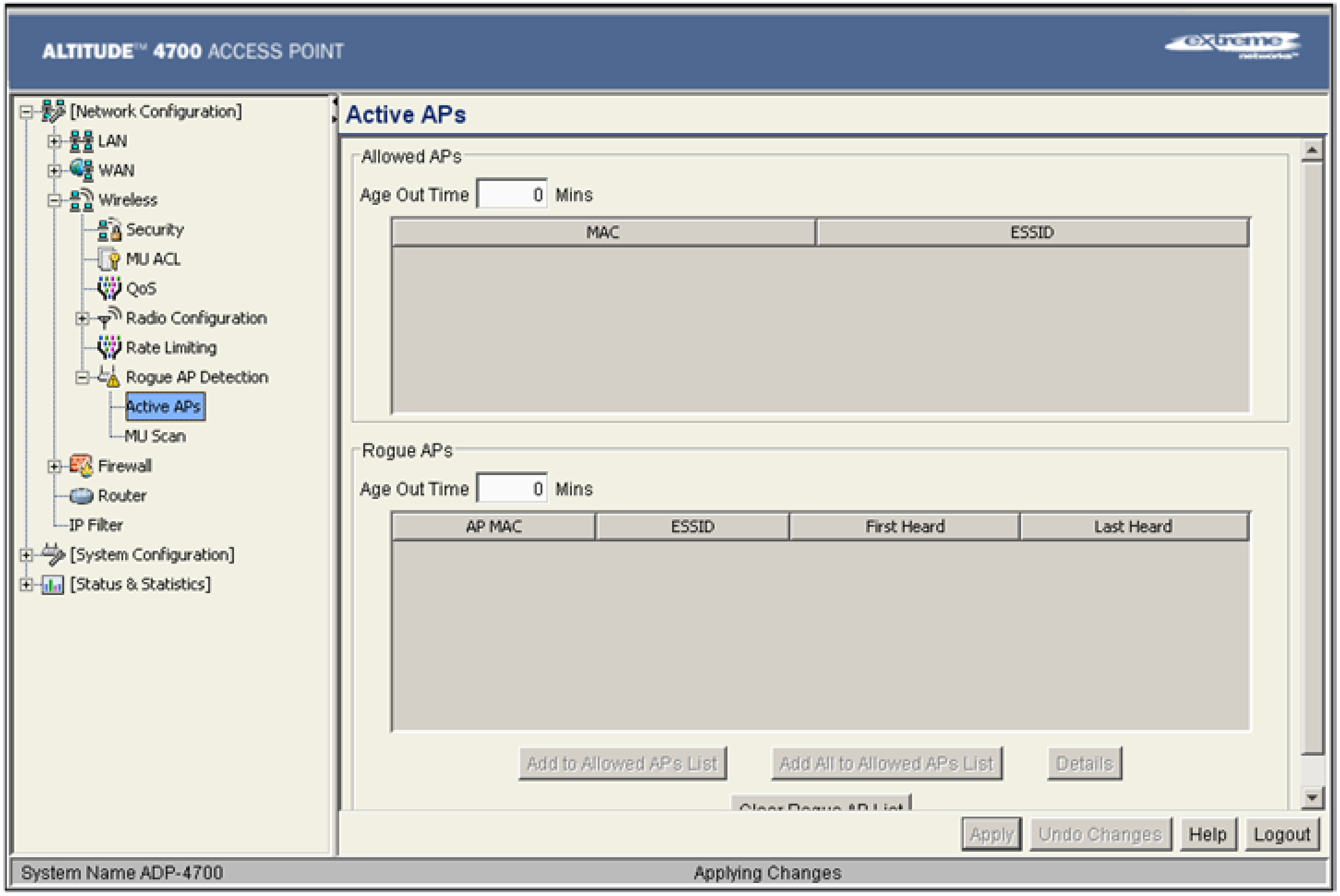
6 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Moving Rogue APs to the Allowed AP List

The *Active APs* screen enables the user to view the list of detected rogue APs and, if necessary, select and move an AP into a list of allowed devices. This is helpful when the settings defined within the *Rogue AP Detection* screen inadvertently detect and define a device as a rogue AP.

To move detected rogue APs into a list of allowed APs:

1 Select *Network Configuration > Wireless > Rogue AP Detection > Active APs* from the access point menu tree.



Active APs

Allowed APs

Age Out Time 0 Mins

MAC	ESSID

Rogue APs

Age Out Time 0 Mins

AP MAC	ESSID	First Heard	Last Heard

System Name ADP-4700 Applying Changes

The Active APs screen displays with detected rogue devices displayed within the *Rogue APs* table.

2 Enter a value (in minutes) in the Allowed APs *Age Out Time* field to indicate the number of elapsed minutes before an AP will be removed from the approved list and reevaluated. A zero (0) for this value (default value) indicates an AP can remain on the approved AP list permanently.

3 Enter a value (in minutes) in the Rogue APs *Age Out Time* field to indicate the number of elapsed minutes before an AP will be removed from the rogue AP list and reevaluated. A zero (0) for this value (default value) indicates an AP can remain on the rogue AP list permanently.

4 Highlight an AP from within the Rogue APs table and click the *Add to Allowed APs List* button to move the device into the list of Allowed APs.

5 Click the *Add All to Allowed APs List* button to move each of the APs displayed within the Rogue APs table to the list of allowed APs.

6 Highlight a rogue AP and click the *Details* button to display a screen with device and detection information specific to that rogue device. This information is helpful in determining if a rogue AP should be moved to the Allowed APs table.

For more information on the displaying information on detected rogue APs, see "Displaying Rogue AP Details" on page 247.

7 To remove the Rogue AP entries displayed within the Rogue APs field, click the *Clear Rogue AP List* button.

Extreme Networks only recommends clearing the list of Rogue APs when the devices displaying within the list do not represent a threat to the Access Point managed network.

8 Click *Apply* to save any changes to the Active APs screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.

9 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Active APs screen to the last saved configuration.

10 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Displaying Rogue AP Details

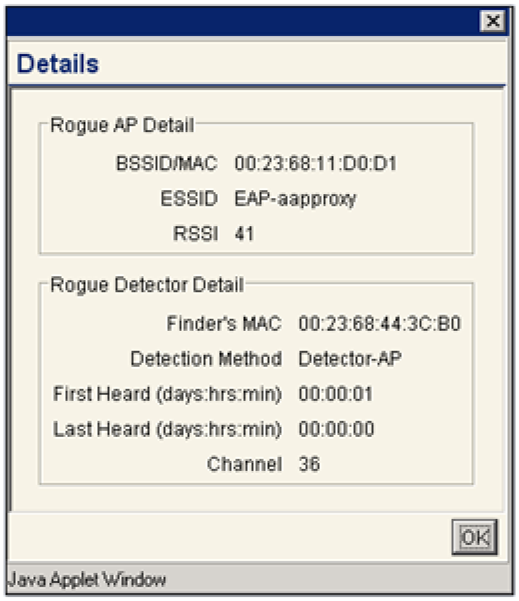
Before moving a rogue AP into the list of allowed APs within the Active APs screen, the device address and rogue detection information for that AP should be evaluated.

To evaluate the properties of a rogue AP:

1 Select *Network Configuration* > *Wireless* > *Rogue AP Detection* > *Active APs* from the access point menu tree.

2 Highlight a target rogue AP from within Rogue APs table and click the *Details* button.

The *Detail* screen displays for the rogue AP.



Details

Rogue AP Detail

BSSID/MAC	00:23:68:11:D0:D1
ESSID	EAP-aapproxy
RSSI	41

Rogue Detector Detail

Finder's MAC	00:23:68:44:3C:B0
Detection Method	Detector-AP
First Heard (days:hrs:min)	00:00:01
Last Heard (days:hrs:min)	00:00:00
Channel	36

3 Refer to the *Rogue AP Detail* field for the following information:

BSSID/MAC	Displays the MAC address of the rogue AP. This information could be useful if the MAC address is determined to be an Extreme Networks MAC address and the device is interpreted as non-hostile and the device should be defined as an allowed AP.
ESSID	Displays the ESSID of the rogue AP. This information could be useful if the ESSID is determined to be non-hostile and the device should be defined as an allowed AP.
RSSI	Shows the *Relative Signal Strength* (RSSI) of the rogue AP. Use this information to assess how close the rogue AP is. The higher the RSSI, the closer the rogue AP. If multiple Access Point's have detected the same rogue AP, RSSI can be useful in triangulating the location of the rogue AP.

4 Refer to the *Rogue Detector Detail* field for the following information:

Finder's MAC	The MAC address of the Access Point detecting the rogue AP.
Detection Method	Displays the *RF Scan by MU*, *RF On-Channel Detection* or *RF Scan by Detector Radio* method selected from the Rogue AP screen to detect rogue devices. For information on detection methods, see "Configuring Rogue AP Detection" on page 243.
First Heard (days:hrs:min)	Defines the time in (days:hrs:min) that the rogue AP was initially heard by the detecting AP.
Last Heard (days:hrs:min)	Defines the time in (days:hrs:min) that the rogue AP was last heard by the detecting AP.
Channel	Displays the channel the rogue AP is using.

5 Click *OK* to securely exit the Detail screen and return to the Active APs screen.

6 Click *Cancel* (if necessary) to undo any changes made and return to the Active APs screen.

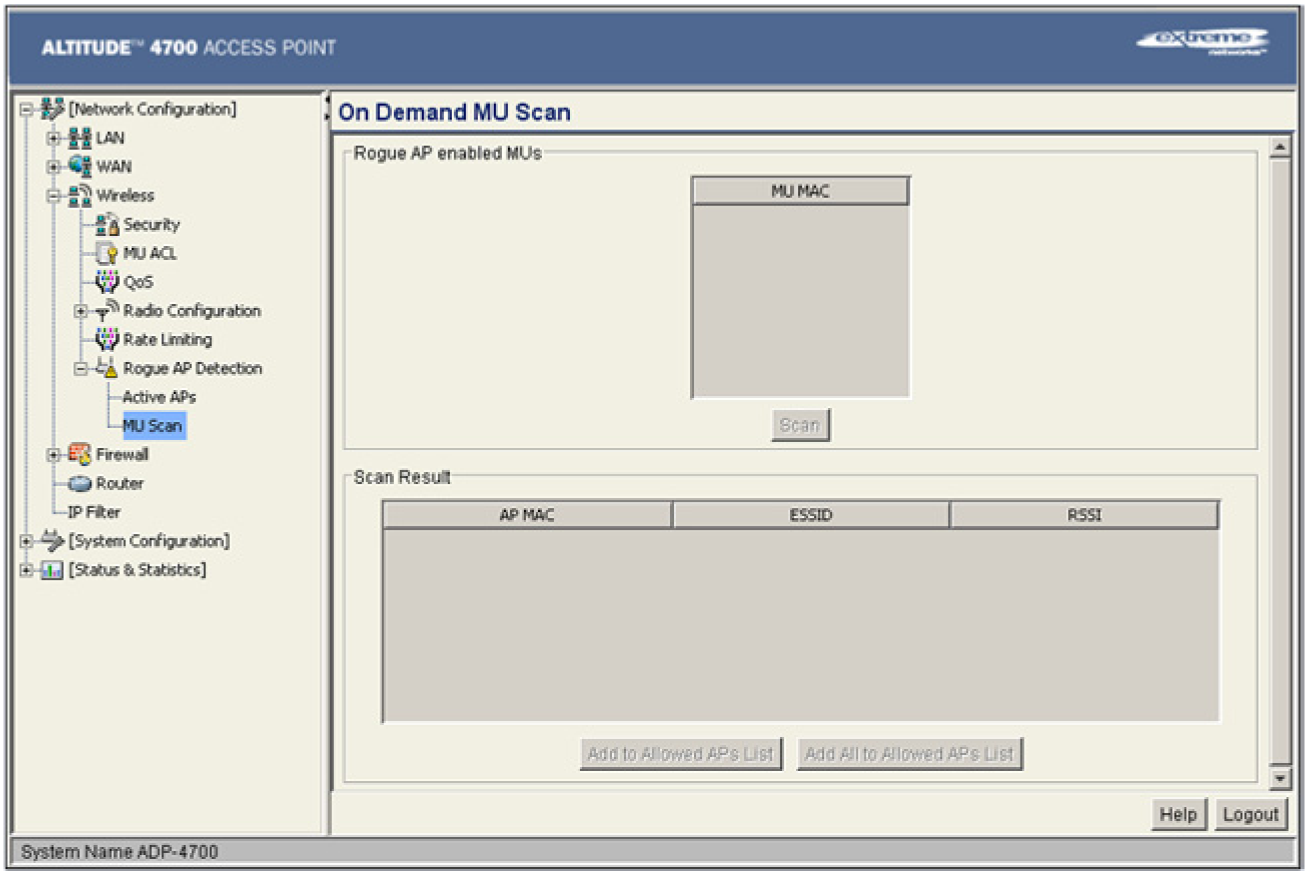
Using MUs to Detect Rogue Devices

The Access Point can use an associated MU that has its rogue AP detection feature enabled to scan for rogue APs. Once detected, the rogue AP(s) can be moved to the list of allowed devices (if appropriate) within the Active APs screen. When adding an MU's detection capabilities with the Access Point's own rogue AP detection functionality, the rogue detection area can be significantly extended.

To use associated rogue AP enabled MUs to scan for rogue APs:

1 Select *Network Configuration* > *Wireless* > *Rogue AP Detection* > *MU Scan* from the access point menu tree.

The *On Demand MU Scan* screen displays with associated MUs with rogue AP detection enabled



2 Highlight an MU from within the *Rogue AP enabled MUs* field and click the scan button.

The target MU begins scanning for rogue devices using the detection parameters defined within the Rogue AP Detection screen. To modify the detection parameters, see "Configuring Rogue AP Detection" on page 243.

Those devices detected as rogue APs display within the *Scan Result* table. Use the displayed AP MAC, ESSID and RSSI values to determine the device listed in the table is truly a rogue device or one inadvertently detected as a rogue AP.

3 If necessary, highlight an individual MU from within the Scan Result field and click the *Add to Allowed AP List* button to move the AP into the Allowed APs table within the *Active APs* screen.

4 Additionally, if necessary, click the *Add All to Allowed APs List* button to move every device within the Scan Result table into the Allowed APs table within the *Active APs* screen. Only use this option if

you are sure all of the devices detected and displayed within the Scan Results table are non-hostile APs.

5 Highlight a different MU from the Rogue AP enabled MUs field as needed to scan for additional rogue APs.

6 Click *Logout* to return to the Rogue AP Detection screen.

Configuring User Authentication

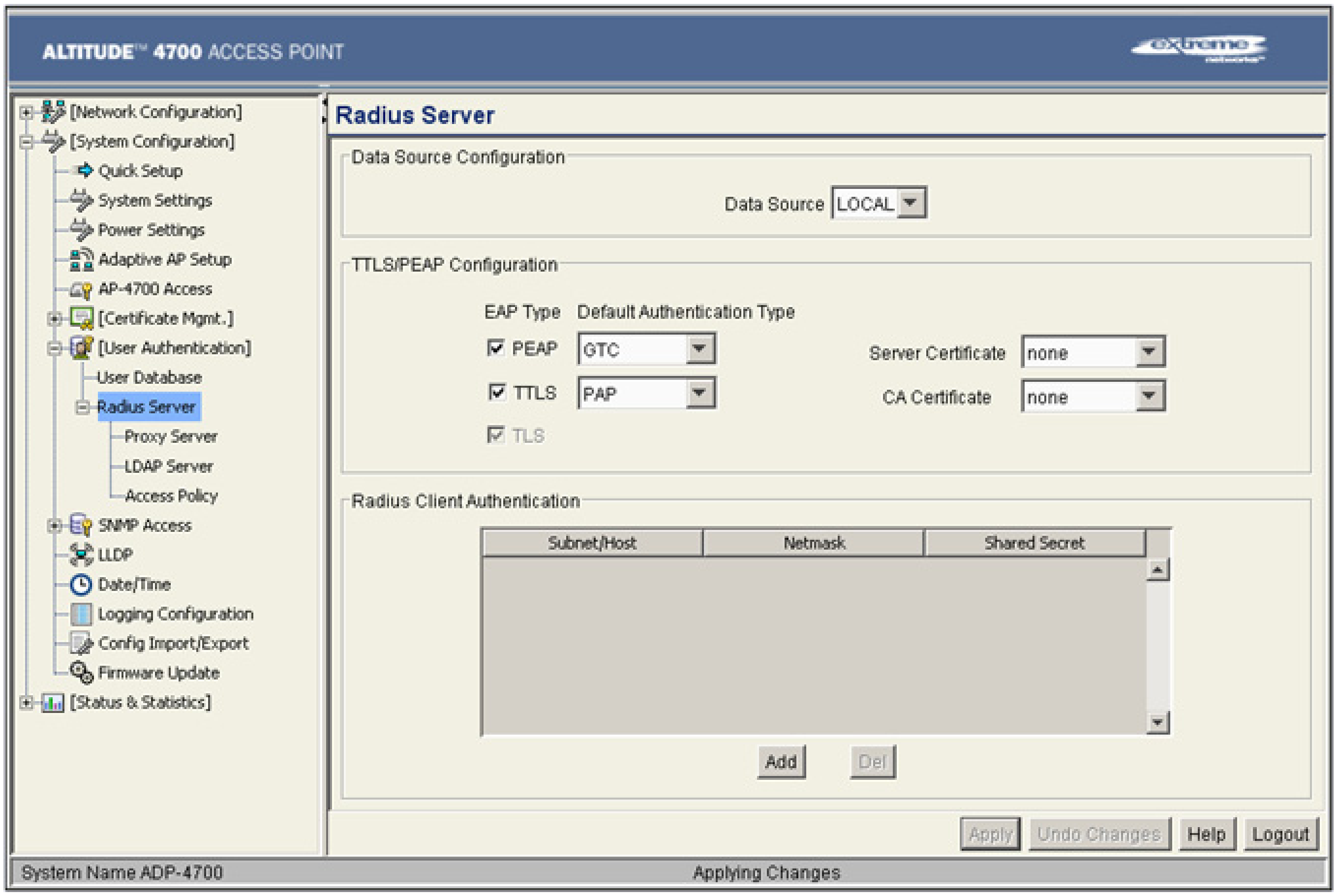
The Access Point can work with external RADIUS and LDAP Servers (AAA Servers) to provide user database information and user authentication.

Configuring the Radius Server

The *Radius Server* screen enables an administrator to define data sources and specify authentication information for the RADIUS Server.

To configure the RADIUS Server:

1 Select *System Configuration* > *User Authentication* > *Radius Server* from the menu tree.



Radius Server

Data Source Configuration

Data Source: LOCAL

TTLS/PEAP Configuration

EAP Type	Default Authentication Type
☑ PEAP	GTC
☑ TTLS	PAP
☑ TLS	

Server Certificate: none

CA Certificate: none

Radius Client Authentication

Subnet/Host	Netmask	Shared Secret

System Name ADP-4700

Applying Changes

2 From within the *Data Source Configuration* field, use the *Data Source* drop-down menu to select the data source for the RADIUS server.

Local

An internal user database serves as the data source. Use the *User Database* screen to enter the user data. For more information, see “Managing the Local User Database” on page 257.

LDAP

If LDAP is selected, the controller will use the data in an LDAP server. Configure the LDAP server settings on the LDAP screen under RADIUS Server on the menu tree. For more information, see “Configuring LDAP Authentication” on page 253.

NOTE

When using LDAP, only PEAP-GTC and TTLS/PAP are supported.

3 Use the *TTLS/PEAP Configuration* field to specify the RADIUS Server default EAP type, EAP authentication type and a Server or CA certificate (if used).

EAP Type

Use the *EAP Type* checkboxes to enable the default EAP type(s) for the RADIUS server. Options include:

- *PEAP*—Select the PEAP checkbox to enable both PEAP types (GTC and MSCHAP-V2) available to the Access Point. PEAP uses a TLS layer on top of EAP as a carrier for other EAP modules. PEAP is an ideal choice for networks using legacy EAP authentication methods.
- *TTLS*—Select the TTLS checkbox to enable all three TTLS types (MD5, PAP and MSCHAP-V2) available to the Access Point.TTLS is similar to EAP-TLS, but the client authentication portion of the protocol is not performed until after a secure transport tunnel is established. This allows EAP-TTLS to protect legacy authentication methods used by some RADIUS servers.
- *TLS*—The TLS checkbox is selected but disabled by default and resides in the background as it does not contain user configurable parameters.

Default Authentication Type — Specify a PEAP and/or TTLS Authentication Type for EAP to use from the drop-down menu to the right of each checkbox item. PEAP options include:

- *GTC—EAP Generic Token Card* (GTC) is a challenge handshake authentication protocol using a hardware token card to provide the response string.
- *MSCHAP-V2—Microsoft CHAP* (MSCHAP-V2) is an encrypted authentication method based on Microsoft's challenge/response authentication protocol.

TTLS options include:

- *PAP—Password Authentication Protocol* sends a username and password over a network to a server that compares the username and password to a table of authorized users. If the username and password are matched in the table, server access is authorized. WatchGuard products do not support the PAP protocol because the username and password are sent as clear text that a hacker can read.
- *MD5*—This option enables the MD5 algorithm for data verification. MD5 takes as input a message of arbitrary length and produces a 128- bit fingerprint. The MD5 algorithm is intended for digital signature applications, in which a large file must be compressed in a secure manner before being encrypted with a private (secret) key under a public-key cryptographic system.
- *MSCHAP-V2—Microsoft CHAP* (MSCHAP-V2) is an encrypted authentication method based on Microsoft's challenge/response authentication protocol.

Server Certificate — If you have a server certificate from a CA and wish to use it on the RADIUS server, select it from the drop-down menu. Only certificates imported to the Access Point are available in the menu.

CA Certificate — You can also choose an imported CA Certificate to use on the RADIUS server. If using a server certificate signed by a CA, import that CA's root certificate using the CA certificates screen. After a valid CA certificate has been imported, it is available from the CA Certificate drop-down menu.

CAUTION

If you have imported a Server or CA certificate, the certificate will not be saved when updating the Access Point’s firmware. Export your certificates before upgrading the Access Point’s firmware. From the Access Point CLI, use the admin(system.cmgr)> expcert command to export the certificate to a secure location.

4 Use the *Radius Client Authentication* table to configure multiple shared secrets based on the subnet or host attempting to authenticate with the RADIUS server. Use the *Add* button to add entries to the list. Modify the following information as needed within the table.

Subnet/Host — Defines the IP address of the subnet or host that will be authenticating with the RADIUS server. If a WLAN has been created to support mesh networking, then enter the IP address of mesh client bridge in order for the MU to authenticate with a base bridge.

Netmask — Defines the netmask (subnet mask) of the subnet or host authenticating with the RADIUS server.

Shared Secret	Click the Passwords button and set a shared secret used for each host or subnet authenticating against the RADIUS server. The shared secret can be up to 7 characters in length.

5 Click *Apply* to save any changes to the RADIUS Server screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.

6 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the RADIUS Server screen to the last saved configuration.

7 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring LDAP Authentication

When the RADIUS Data Source is set to use an external LDAP server (see "Configuring the Radius Server" on page 250), the *LDAP* screen is used to configure the properties of the external LDAP server.

To configure the LDAP server:

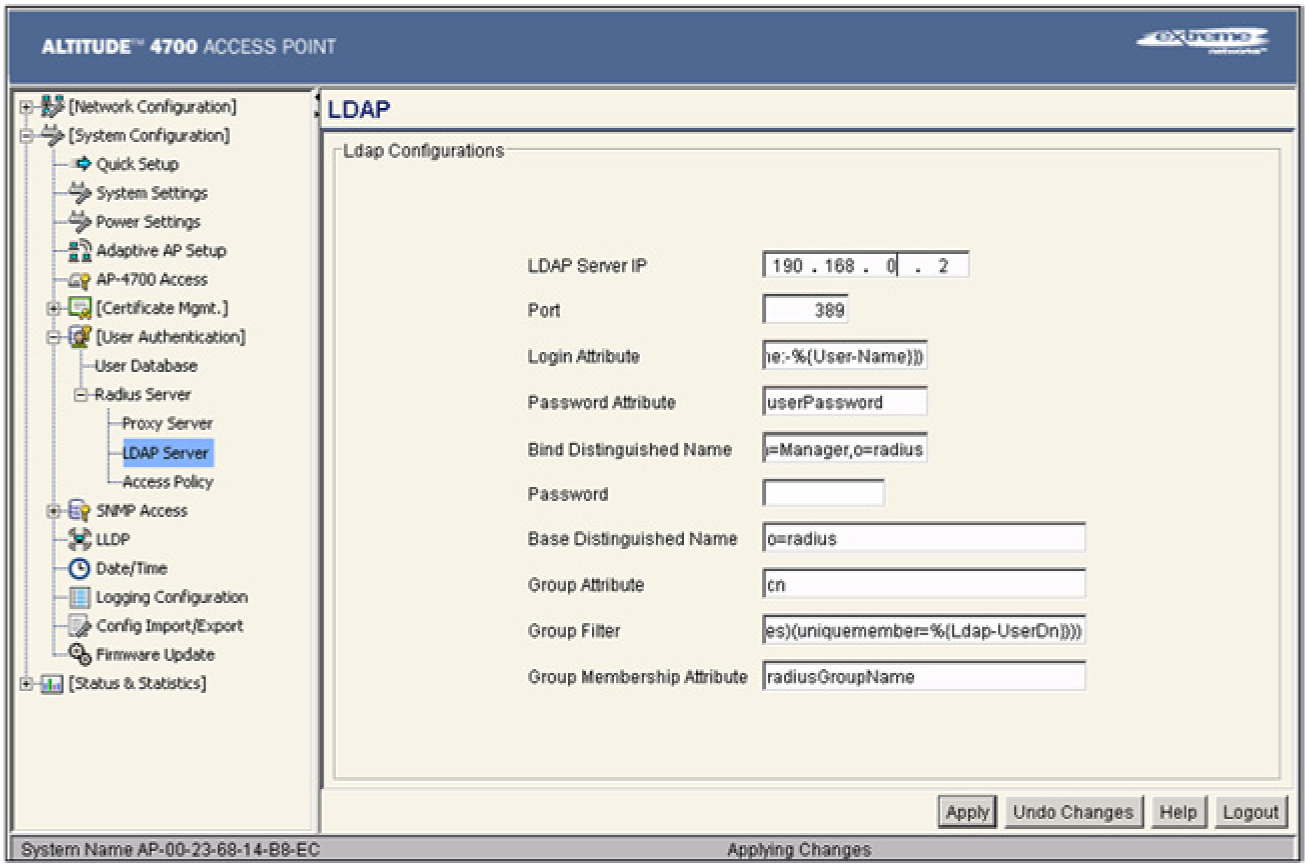
1 Select *System Configuration* > *User Authentication* > *RADIUS Server* > *LDAP* from the menu tree.

NOTE

For the onboard RADIUS server to work with Windows Active Directory or open LDAP as the database, the user has to be present in a group within the organizational unit. The same group must be present within the onboard RADIUS server's database. The group configured within the onboard RADIUS server is used for group policy configuration to support a new Time Based Rule restriction feature.

NOTE

The LDAP screen displays with unfamiliar alphanumeric characters (if new to LDAP configuration). Extreme Networks recommends only qualified administrators change the default values within the LDAP screen.



LDAP

Ldap Configurations

LDAP Server IP	190 . 168 . 0 . 2
Port	389
Login Attribute	ne:-%{User-Name}})
Password Attribute	userPassword
Bind Distinguished Name	=Manager,o=radius
Password	
Base Distinguished Name	o=radius
Group Attribute	cn
Group Filter	es)(uniquemember=%{Ldap-UserDn})))
Group Membership Attribute	radiusGroupName

2 Enter the appropriate information within the LDAP Configuration field to allow the Access Point to interoperate with the LDAP server. Consult with your LDAP server administrator for details on how to define the values in this screen.

LDAP Server IP

Enter the IP address of the external LDAP server acting as the data source for the RADIUS server. The LDAP server must be accessible from the WAN port or from the Access Point's active subnet.

Port

Enter the TCP/IP port number for the LDAP server acting as a data source for the RADIUS. The default port is 389.

Login Attribute

Specify the login attribute used by the LDAP server for authentication. In most cases, the default value should work. Windows Active Directory users must use "sAMAccountName" as their login attribute to successfully login to the LDAP server.

Password Attribute

Enter the password used by the LDAP server for authentication.

Bind Distinguished Name

Specify the distinguished name used to bind with the LDAP server.

Password

Enter a valid password for the LDAP server.

Base Distinguished Name

Enter a name that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching.

Group Attribute

Define the group attribute used by the LDAP server.

Group Filter

Specify the group filters used by the LDAP server.

Group Member Attribute	Enter the Group Member Attribute sent to the LDAP server when authenticating users.

CAUTION

Windows Active Directory users must set their Login Attribute to “sAMAccountName” in order to successfully login to the LDAP server.

3 Click *Apply* to save any changes to the LDAP screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.

4 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the LDAP screen to the last saved configuration.

5 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring a Proxy Radius Server

The Access Point has the capability to proxy authentication requests to a remote RADIUS server based on the suffix of the user ID (such as myisp.com or company.com). The Access Point supports up to 10 proxy servers.

CAUTION

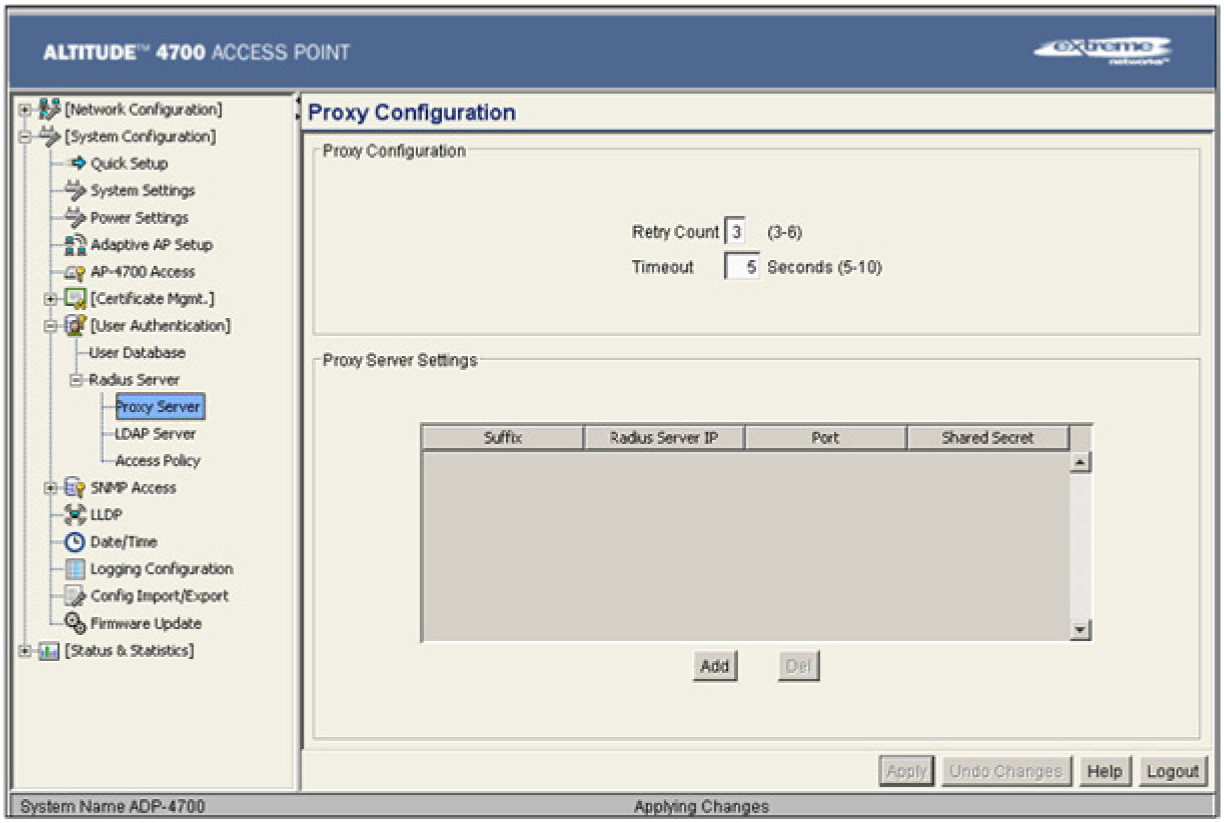
If using a proxy server for RADIUS authentication, the Data Source field within the RADIUS server screen must be set to Local. If set to LDAP, the proxy server will not be successful when performing the authentication. To verify the existing settings, see “Configuring the Radius Server” on page 250.

CAUTION

When configuring the credentials of an MU, ensure its login (or user) name is a Fully Qualified Domain Name (FQDN), or it cannot be authenticated by the Access Point’s proxy server. For example: ap4700@2kserver.FUSCIA.com.

To configure the proxy RADIUS server for the access point:

1 Select *System Configuration* > *User Authentication* > *Radius Server* > *Proxy* from the menu tree.



Proxy Configuration

Proxy Configuration

Retry Count 3 (3-6)

Timeout 5 Seconds (5-10)

Proxy Server Settings

Suffix	Radius Server IP	Port	Shared Secret

System Name ADP-4700

Applying Changes

2 Refer to the *Proxy Configuration* field to define the proxy server's retry count and timeout values.

Retry Count Enter a value between 3 and 6 to indicate the number of times the Access Point attempts to reach a proxy server before giving up.

Timeout Enter a value between 5 and 10 to indicate the number of elapsed seconds causing the Access Point to time out on a request to a proxy server.

3 Use the *Add* button to add a new proxy server. Define the following information for each entry:

Suffix Enter the domain suffix (such as myisp.com or mycompany.com) of the users sent to the specified proxy server.

Radius Server IP Specify the IP address of the RADIUS server acting as a proxy server.

Port Enter the TCP/IP port number for the RADIUS server acting as a proxy server. The default port is 1812.

Shared Secret Set a shared secret used for each suffix used for authentication with the RADIUS proxy server.

4 To remove a row, select the row and click the *Del* (Delete) button.

5 Click *Apply* to save any changes to the Proxy screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.

6 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Proxy screen to the last saved configuration.

7 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Managing the Local User Database

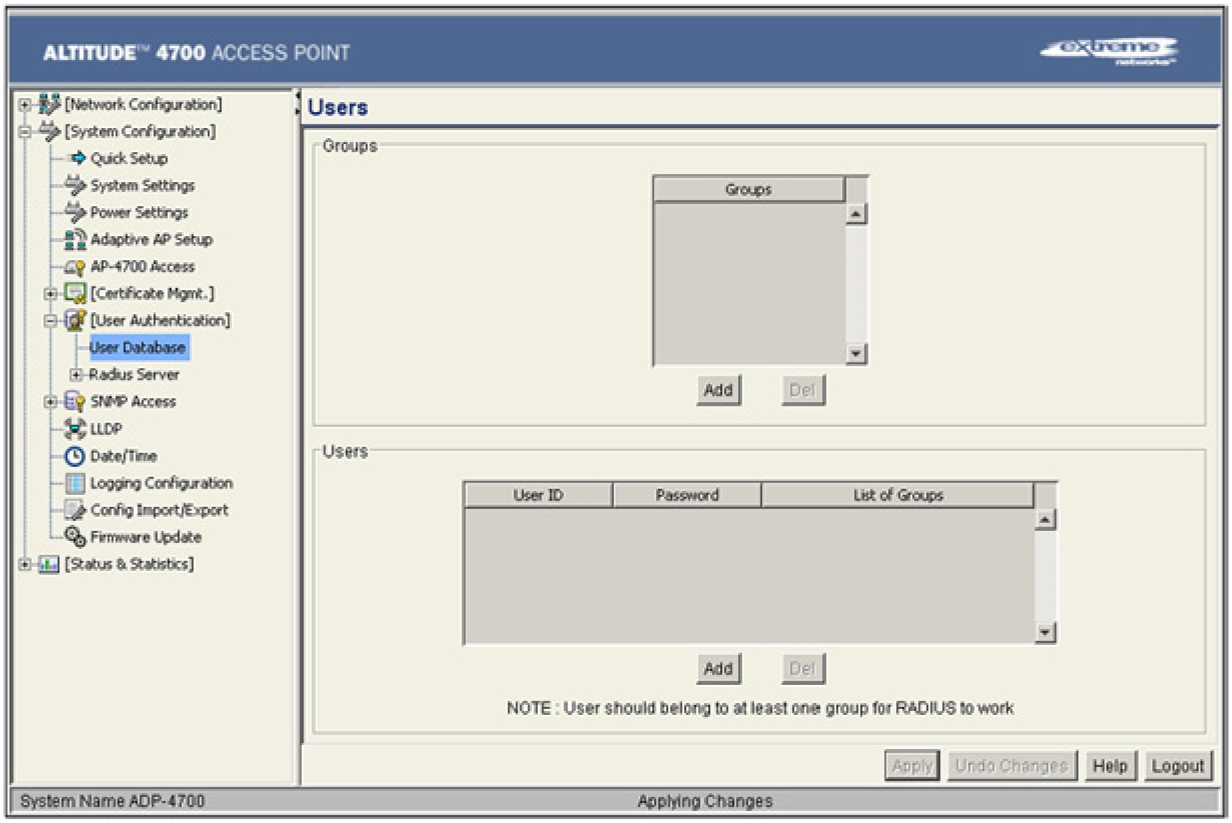
Use the *User Database* screen to create groups for use with the RADIUS server. The database of groups is employed if *Local* is selected as the Data Source from the RADIUS Server screen. For information on selecting Local as the Data Source, see "Configuring the Radius Server" on page 250.

To add groups to the User database:

NOTE

Each group can be configured to have its own access policy using the Access Policy screen. For more information, see "Defining User Access Permissions by Group" on page 259.

1 Select *System Configuration* > *User Authentication* > *User Database* from the menu tree.



NOTE : User should belong to at least one group for RADIUS to work

System Name ADP-4700 Applying Changes

Refer to the *Groups* field for a list of all groups in the local RADIUS database. The groups are listed in the order added. Although groups can be added and deleted, there is no capability to edit a group name.

2 Click the *Add* button and enter the name of the group in the new blank field in the Groups table.

3 To remove a group, select the group from the table and click the *Del* (Delete) key.

The *Users* table displays the entire list of users. Up to 100 users can be entered here. The users are listed in the order added. Users can be added and deleted, but there is no capability to edit the name of a group.

4 To add a new user, click the *Add* button at the bottom of the Users area.

5 In the new line, type a *User ID* (username).

6 Click the *Password* cell. A small window displays. Enter a password for the user and click *OK* to return to the Users screen.

7 Click the *List of Groups* cell. A new screen displays enabling you to associate groups with the user. For more information on mapping groups with a user, see "Mapping Users to Groups" on page 258.

8 Click *Apply* to save any changes to the Users screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.

9 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Users screen to the last saved configuration.

10 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Mapping Users to Groups

Once users have been created within the *Users* screen, their access privileges need to be configured for inclusion to one, some or all of the groups also created within the Users screen.

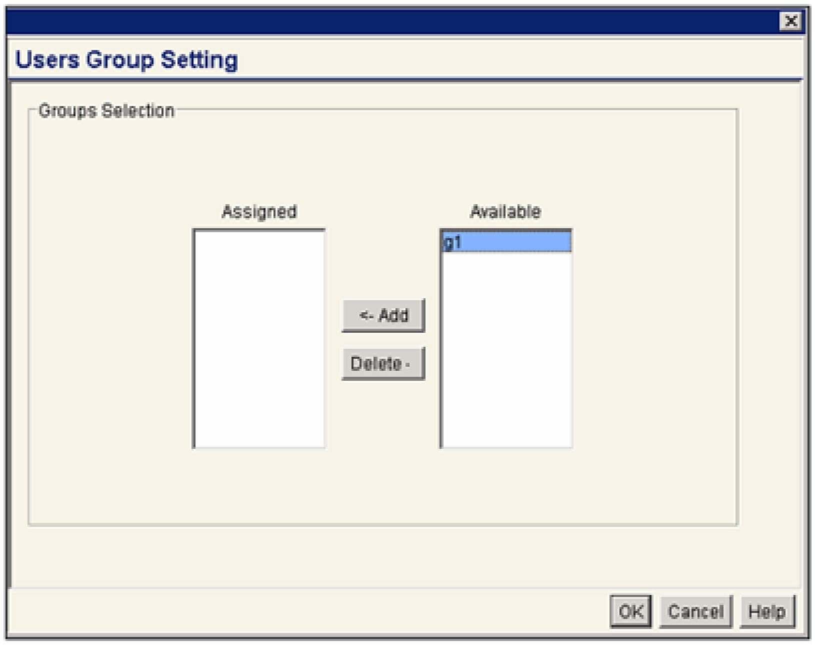
To map users to groups for group authentication privileges:

1 If you are not already in the Users screen, select *System Configuration* > *User Authentication* > *User Database* from the menu tree.

Existing users and groups display within their respective fields. If user or group requires creation or modification, make your changes before you begin to map them.

2 Refer to the Users field and select the *List of Groups* column for the particular user you wish to map to one or more groups.

The *Users Group Setting* screen displays with the groups available for user inclusion displayed within the *Available* column.



3 To add the user to a group, select the group in the *Available* list (on the right) and click the *<-Add* button.

Assigned users will display within the *Assigned* table. Map one or more groups as needed for group authentication access for this particular user.

4 To remove the user from a group, select the group in the Assigned list (on the left) and click the *Delete ->* button.

5 Click the *OK* button to save your user and group mapping assignments and return to the Users screen.

Defining User Access Permissions by Group

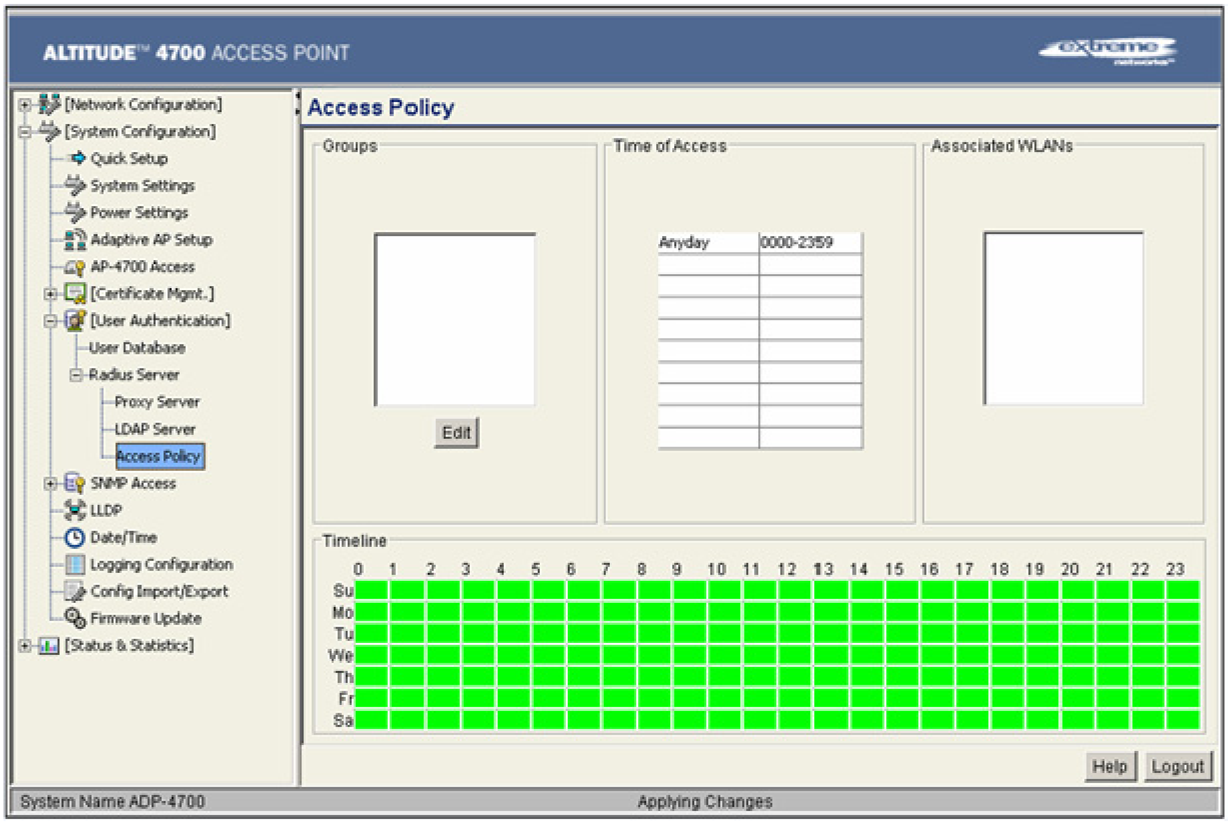
An external AAA server maintains the users and groups database used by the Access Point for access permissions. Various kinds of access policies can be applied to each group. Individual groups can be associated with their own time-based access policy. Each group's policy has a user defined interval defining the days and hours access is permitted. Authentication requests for users belonging to the group are honored only during these defined hourly intervals.

Refer to the *Access Policy* screen to define WLAN access for the user group(s) defined within the Users screen. Each group created within the Users screen displays in the Access Policy screen within the groups column. Similarly, existing WLANs can be individually mapped to user groups by clicking the WLANs button to the right of each group name. For more information on creating groups and users, see "Managing the Local User Database" on page 257. For information on creating a new WLAN or editing the properties of an existing WLAN, see "Creating/Editing Individual WLANs" on page 148.

CAUTION

If using the RADIUS time-based authentication feature to authenticate Access Point user permissions, ensure UTC has been selected from the Date and Time Settings screen's Time Zone field. If UTC is not selected, time based authentication will not work properly. For information on setting the time zone for the Access Point, see "Configuring Network Time Protocol (NTP)" on page 110.

1 Select *User Authentication > Radius Server > Access Policy* from the menu tree.



Anyday	0000-2359

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Su	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Mo	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Tu	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
We	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Th	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Fr	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Sa	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

The Access Policy screen displays the following fields:

Groups — The *Groups* field displays the names of those existing groups that can have access intervals applied to them. Click the *Edit* button to display a screen designed to create access intervals for specific days and hours. A mechanism also exists for mapping specific WLANs to these intervals. For more information, see "Editing Group Access Permissions" on page 261. For information on creating a new group, see "Managing the Local User Database" on page 257.

Time of Access — The *Time of Access* field displays the days of the week and the hours defined for group access to Access Point resources. This data is defined for the group by selecting the *Edit* button from within the *groups* field.

Associated WLANs — The *Associated WLANs* field displays the WLANs assigned the user group access permissions listed within the filters and grid fields. Add additional WLANs to a group by selecting the Edit button within the groups field.

grid — Refer to the *grid* field to review a bar graph of the selected group's access privileges. Revise the selected group's privileges as needed to

2 Review the existing access intervals assigned to each group by selecting the group from amongst those displayed. To modify a group’s permissions, see “Editing Group Access Permissions” on page 261.

3 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Editing Group Access Permissions

The Access Policy screen provides a mechanism for modifying an existing group’s access permissions. A group’s permissions can be set for any day of the week and include any hour of the day. Ten unique access intervals can be defined for each existing group.

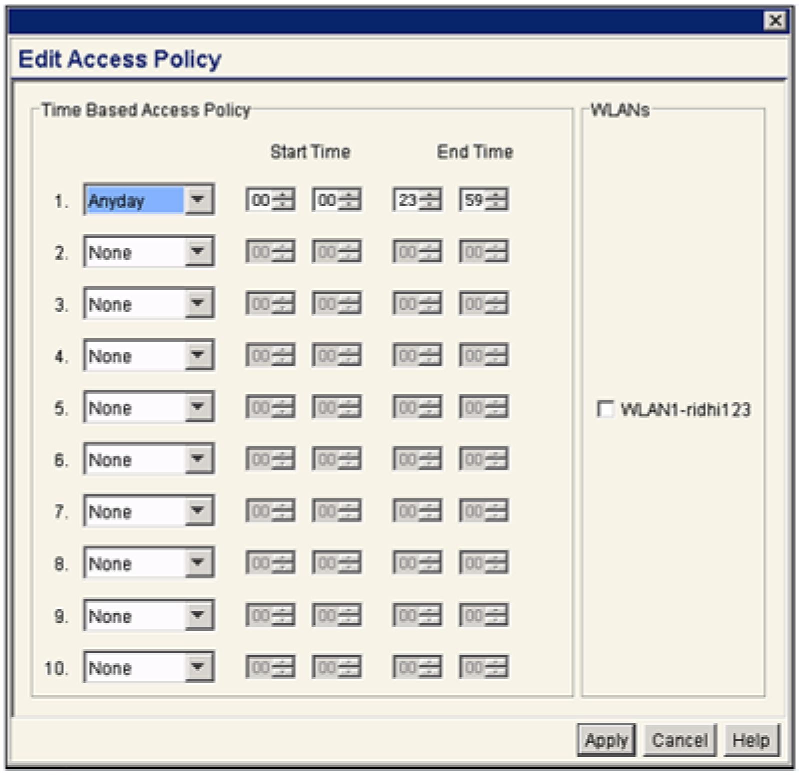
To update a group’s access permissions:

1 Select *User Authentication* > *Radius Server* > *Access Policy* from the menu tree.

2 Select an existing group from within the groups field.

3 Select the *Edit* button.

The Edit Access Policy screen displays.



Edit Access Policy

Time Based Access Policy

		Start Time		End Time	
1.	Anyday	00	00	23	59
2.	None	00	00	00	00
3.	None	00	00	00	00
4.	None	00	00	00	00
5.	None	00	00	00	00
6.	None	00	00	00	00
7.	None	00	00	00	00
8.	None	00	00	00	00
9.	None	00	00	00	00
10.	None	00	00	00	00

WLANs

☐ WLAN1-ridhi123

4 Define up to 10 access policies for the selected group within the *Time Based Access Policy* field.

Use the drop-down menus on the left-hand side of the screen to define the day of the week for which each policy applies. If continual access is required, select the *All Days* option. If continual access is required during Monday through Friday, but not Saturday or Sunday, select the *Weekdays* option.

Use the *Start Time* and *End Time* values to define the access interval (in HHMM format) for each access policy. Each policy for a given group should have unique intervals. Policies can be created for different intervals on the same day of the week.

NOTE

Groups have a strict start and end time (as defined using the Edit Access Policy screen). Only during this period of time can authentication requests from users be honored (with no overlaps). Any authentication request outside of this defined interval is denied regardless of whether a user's credentials match or not.

5 Refer to the *WLANs* field to select existing WLANs to apply to the selected group's set of access permissions.

The group's existing WLANs are already selected within the Edit screen. Select those additional WLANs requiring the access permissions specified in options 1-10 within the Time Based Access Policy field.

6 Click *Apply* to save any changes to the Edit Access Policy screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.

7 Click *Cancel* if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Edit Access Policy screen to the last saved configuration.

7

CHAPTER

Monitoring Statistics

The access point has functionality to display robust transmit and receive statistics for its WAN and LAN port. *Wireless Local Area Network (WLAN)* stats can also be displayed collectively for each enabled WLAN as well as individually for up to 16 specific WLANs.

Transmit and receive statistics can also be displayed for the access point's 802.11a/n and 802.11b/g/n radios. An advanced radio statistics page is also available to display retry histograms for specific data packet retry information.

Associated MU stats can be displayed collectively for associated MUs and individually for specific MUs. An echo (ping) test is also available to ping specific MUs to assess the strength of the AP association.

Finally, the access point can detect and display the properties of other APs detected within the access point radio coverage area. The type of AP detected can be displayed as well as the properties of individual APs.

See the following sections for more details on viewing statistics for the access point:

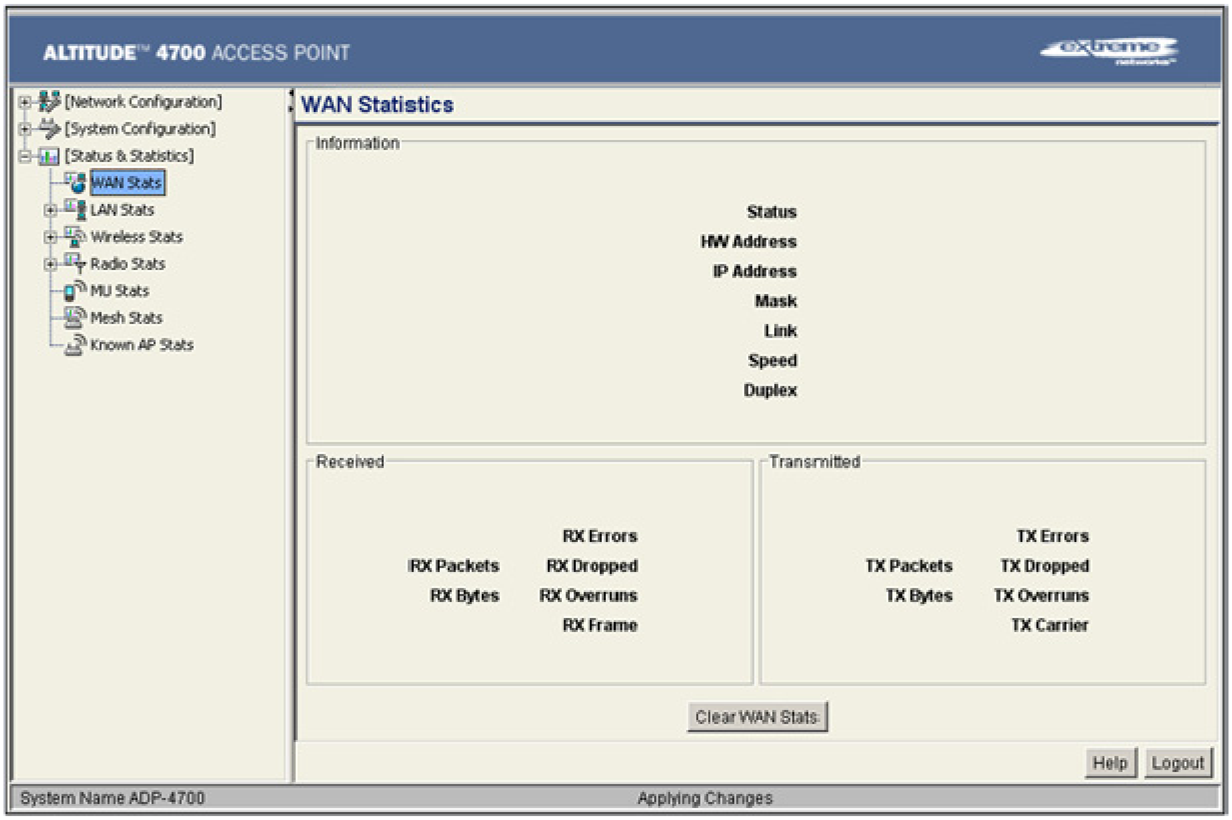
Viewing WAN Statistics

Use the access point *WAN Stats* screen to view real-time statistics for monitoring the access point activity through its *Wide Area Network (WAN)* port.

The *Information* field of the WAN Stats screen displays basic WAN information, generated from settings on the WAN screen. The *Received* and *Transmitted* fields display statistics for the cumulative packets, bytes, and errors received and transmitted through the WAN interface since it was last enabled or the AP was last rebooted. The access point *WAN Stats* screen is view-only with no configurable data fields.

To view access point WAN Statistics:

1 Select *Status and Statistics* > *WAN Stats* from the access point menu tree.



2 Refer to the *Information* field to reference the following access point WAN data:

Status — The *Status* field displays *Enabled* if the WAN interface is enabled on the *WAN* screen. If the WAN interface is disabled on the WAN screen, the WAN Stats screen displays no connection information and statistics.

HW Address — The *Media Access Control (MAC)* address of the access point WAN port. The WAN port MAC address is hard coded at the factory and cannot be changed.

IP Addresses — The displayed *Internet Protocol (IP)* addresses for the access point WAN port.

Mask — The *Mask* field displays the subnet mask number for the access point's WAN connection. This value is set on the *WAN* screen.

Link — The *Link* parameter displays *Up* if the WAN connection is active between the access point and network, and *Down* if the WAN connection is interrupted or lost. Use this information to assess the current connection status of the WAN port.

Speed — The WAN connection speed is displayed in Megabits per second (Mbps), for example, 54Mbps. If the throughput speed is not achieved, examine the number of transmit and receive errors, or consider increasing the supported data rate.

3 Refer to the *Received* field to reference data received over the access point WAN port.

RX Packets
RX packets are data packets received over the WAN port. The displayed number is a cumulative total since the WAN interface was last enabled or the access point was last restarted.

RX Bytes
RX bytes are bytes of information received over the WAN port. The displayed number is a cumulative total since the WAN interface was last enabled or the Access Point was last restarted.

RX Errors
RX errors include dropped data packets, buffer overruns, and frame errors on inbound traffic. The number of RX errors is a total of *RX Dropped*, *RX Overruns* and *RX Carrier* errors. Use this information to determine performance quality of the current WAN connection.

RX Dropped
The *RX Dropped* field displays the number of data packets that fail to reach the WAN interface. If this number appears excessive, consider a new connection to the device.

RX Overruns
RX overruns are buffer overruns on the WAN connection. RX overruns occur when packets are received faster than the WAN port can handle them. If RX overruns are excessive, consider reducing the data rate.

RX Frame
The *RX Frame* field displays the number of TCP/IP data frame errors received.

4 Refer to the *Transmitted* field to reference data received over the access point WAN port.

TX Packets
TX packets are data packets sent over the WAN connection. The displayed number is a cumulative total since the WAN was last enabled or the access point was last restarted.

TX Bytes
TX bytes are bytes of information sent over the WAN connection. The displayed number is a cumulative total since the WAN interface was last enabled or the access point was last restarted.

TX Errors
TX errors include dropped data packets, buffer overruns, and carrier errors on outbound traffic. The displayed number of TX errors is the total of *TX Dropped*, T*X Overruns* and *TX Carrier* errors. Use this information to assess Access Point location and transmit speed.

TX Dropped
The *TX Dropped* field displays the number of data packets that fail to get sent from the WAN interface.

TX Overruns
TX overruns are buffer overruns on the WAN connection. TX overruns occur when packets are sent faster than the WAN interface can handle. If TX overruns are excessive, consider reducing the data rate.

TX Carrier
The *TX Carrier* field displays the number of TCP/IP data carrier errors.

5 Click the *Clear WAN Stats* button to reset each of the data collection counters to zero in order to begin new data collections. The RX/TX Packets and RX/TX Bytes totals remain at their present values and are not cleared.

Do not clear the WAN stats if currently in an important data gathering activity or risk losing all data calculations to that point.

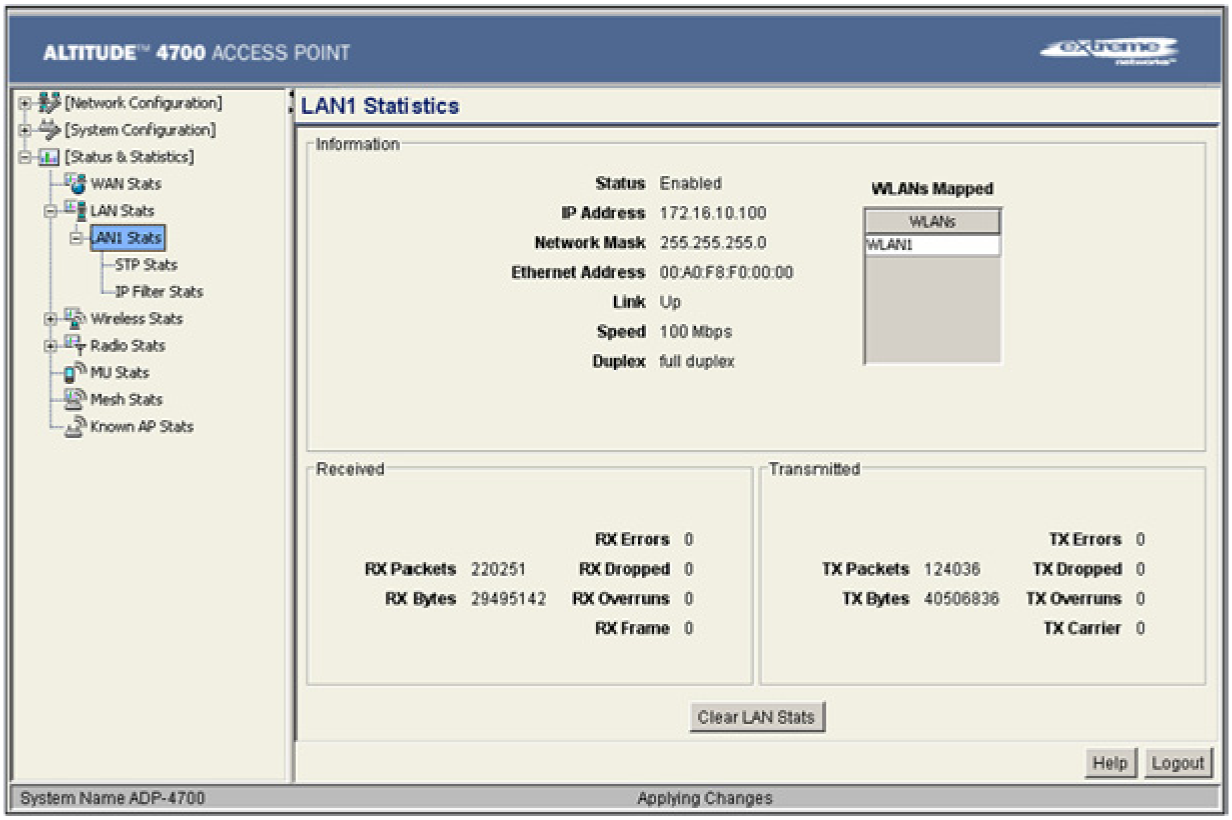
6 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Viewing LAN Statistics

Use the *LAN Stats* screen to monitor the activity of the access point's LAN1 or LAN2 connection. The *Information* field of the LAN Stats screen displays network traffic information as monitored over the access point LAN1 or LAN2 port. The *Received* and *Transmitted* fields of the screen display statistics for the cumulative packets, bytes, and errors received and transmitted over the LAN1 or LAN2 port since it was last enabled or the access point was last restarted. The *LAN Stats* screen is view-only with no user configurable data fields.

To view access point LAN connection stats:

1 Select *Status and Statistics* > *LAN Stats* > *LAN1 Stats* (or LAN2 Stats) from the access point menu tree.



LAN1 Statistics

Information

Status Enabled
IP Address 172.16.10.100
Network Mask 255.255.255.0
Ethernet Address 00:A0:F8:F0:00:00
Link Up
Speed 100 Mbps
Duplex full duplex

WLANs Mapped

WLANs
WLAN1

Received

RX Packets 220251
RX Bytes 29495142
RX Errors 0
RX Dropped 0
RX Overruns 0
RX Frame 0

Transmitted

TX Packets 124036
TX Bytes 40506836
TX Errors 0
TX Dropped 0
TX Overruns 0
TX Carrier 0

System Name ADP-4700 Applying Changes

2 Refer to the *Information* field to view the following access point device address information:

Status
Displays whether this particular LAN has been enabled as viable subnet from within the LAN Configuration screen.

IP Address
The *Internet Protocol (IP)* addresses for the access point LAN port.

Network Mask
The first two sets of numbers specify the network domain, the next set specifies the subset of hosts within a larger network. These values help divide a network into subnetworks and simplify routing and data transmission.

Ethernet Address
The *Media Access Control (MAC)* address of the access point. The MAC address is hard coded at the factory and cannot be changed.

Link

The *Link* parameter displays *Up* if the LAN connection is active between the access point and network, and *Down* if the LAN connection is interrupted or lost. Use this information to assess the current connection status of LAN 1 or LAN2.

Speed

The LAN 1 or LAN 2 connection speed is displayed in Megabits per second (Mbps), for example, 54Mbps. If the throughput speed is not achieved, examine the number of transmit and receive errors, or consider increasing the supported data rate.

Duplex

Displays whether the current LAN connection is full or half duplex.

WLANs Mapped

The *WLANs Mapped* table lists the WLANs mapped to this LAN (either LAN1 or LAN2) as their LAN interface.

3 Refer to the *Received* field to view data received over the access point LAN port.

RX Packets

RX packets are data packets received over the access point LAN port. The number is a cumulative total since the LAN connection was last enabled or the access point was last restarted.

RX Bytes

RX bytes are bytes of information received over the LAN port. The value is a cumulative total since the LAN connection was last enabled or the access point was last restarted.

RX Errors

RX errors include dropped data packets, buffer overruns, and frame errors on inbound traffic. The number of RX errors is a total of *RX Dropped*, *RX Overruns* and *RX Carrier* errors. Use this information to determine performance quality of the current LAN connection.

RX Dropped

The *RX Dropped* field displays the number of data packets failing to reach the LAN port. If this number appears excessive, consider a new connection to the device.

RX Overruns

RX overruns are buffer overruns on the access point LAN port. RX overruns occur when packets are received faster than the LAN connection can handle them. If RX overruns are excessive, consider reducing the data rate.

RX Frame

The *RX Frame* field displays the number of TCP/IP data frame errors received.

4 Refer to the *Transmitted* field to view statistics transmitted over the access point LAN port.

TX Packets

TX packets are data packets sent over the access point LAN port. The displayed number is a cumulative total since the LAN connection was last enabled or the access point was last restarted.

TX Bytes

TX bytes are bytes of information sent over the LAN port. The displayed number is a cumulative total since the LAN Connection was last enabled or the access point was last restarted.

TX Errors

TX errors include dropped data packets, buffer overruns, and carrier errors on outbound traffic. The displayed number of TX errors is a total of *TX Dropped, TX Overruns* and *TX Carrier* errors. Use this information to re-assess AP location and transmit speed.

TX Dropped

The *TX Dropped* field displays the number of data packets that fail to get sent from the access point LAN port.

TX Overruns — TX overruns are buffer overruns on the LAN port. TX overruns occur when packets are sent faster than the LAN connection can handle. If TX overruns are excessive, consider reducing the data rate,

TX Carrier — The *TX Carrier* field displays the number of TCP/IP data carrier errors.

5 Click the *Clear LAN Stats* button to reset each of the data collection counters to zero in order to begin new data collections. The RX/TX Packets and RX/TX Bytes totals remain at their present values and are not cleared.

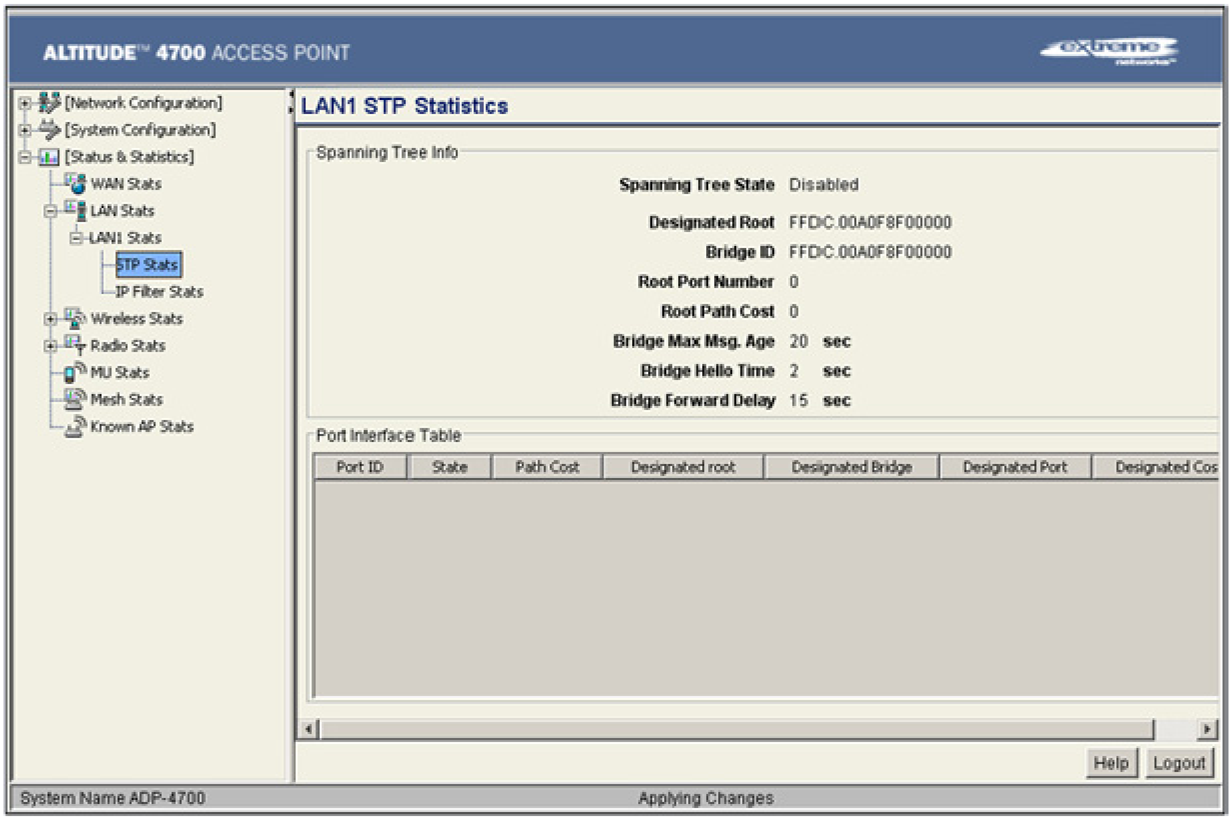
6 Click the *Logout* button to securely exit the Access Point applet. There will be a prompt confirming logout before the applet is closed.

Viewing a LAN's STP Statistics

Each Access Point LAN has the ability to track its own unique STP statistics. Refer to the LAN STP Stats page when assessing mesh networking functionality for each of the two Access Point LANs. Access points in bridge mode exchange configuration messages at regular intervals (typically 1 to 4 seconds). If a bridge fails, neighboring bridges detect a lack of configuration messaging and initiate a spanning-tree recalculation (when spanning tree is enabled).

To view access point LAN's STP statistics:

1 Select *Status and Statistics* > *LAN Stats* > *LAN1 Stats* (or LAN2 Stats) > *STP Stats* from the access point menu tree.



LAN1 STP Statistics

Spanning Tree Info

Spanning Tree State: Disabled
Designated Root: FFDC.00A0F8F00000
Bridge ID: FFDC.00A0F8F00000
Root Port Number: 0
Root Path Cost: 0
Bridge Max Msg. Age: 20 sec
Bridge Hello Time: 2 sec
Bridge Forward Delay: 15 sec

Port Interface Table

Port ID	State	Path Cost	Designated root	Designated Bridge	Designated Port	Designated Cos

System Name ADP-4700 Applying Changes

2 Refer to the *Spanning Tree Info* field to for details on spanning tree state, and root Access Point designation.

Spanning Tree State	Displays whether the spanning tree state is currently enabled or disabled. The spanning tree state must be enabled for a unique spanning-tree calculation to occur when the bridge is powered up or when a topology change is detected.
Designated Root	Displays the Access Point MAC address of the bridge defined as the root bridge in the Bridge STP Configuration screen.
Bridge ID	The Bridge ID identifies the priority and ID of the bridge sending the message
Root Port Number	Identifies the root bridge by listing its 2-byte priority followed by its 6-byte ID.
Root Path Cost	Bridge message traffic contains information identifying the root bridge and the sending bridge. The root path cost represents the distance (cost) from the sending bridge to the root bridge.
Bridge Max Msg. Age	The Max Msg Age measures the age of received protocol information recorded for a port, and to ensure the information is discarded when it exceeds the value set for the Maximum Message age timer. For information on setting the Maximum Message Age.
Bridge Hello Time	The Bridge Hello Time is the time between each bridge protocol data unit sent. This time is equal to 2 seconds (sec) by default, but can tuned between 1 and 10 sec. The 802.1d specification recommends the Hello Time be set to a value less than half of the Max Message age value.
Bridge Forward Delay	The Bridge Forward Delay value is the time spent in a listening and learning state. This time is equal to 15 sec by default, but you can tune the time to be between 4 and 30 sec.

3 Refer to the *Port Interface Table* to assess the state of the traffic over the ports listed within the table for the root and bridge and designated bridges.

Port ID	Identifies the port from which the configuration message was sent.
State	Displays whether a bridge is forwarding traffic to other members of the mesh network (over this port) or blocking traffic. Each viable member of the mesh network must forward traffic to extent the coverage area of the mesh network.
Path Cost	The root path cost is the distance (cost) from the sending bridge to the root bridge.
Designated Root	Displays the MAC address of the Access Point defined with the lowest priority within the Mesh STP Configuration screen.
Designated Bridge	There is only one root bridge within each mesh network. All other bridges are designated bridges that look to the root bridge for several mesh network timeout values.
Designated Port	Each designated bridge must use a unique port. The value listed represents the port used by each bridge listed within the table to route traffic to other members of the mesh network.

Designated Cost	Displays the unique distance between each Access Point MAC address listed in the Designated Bridge column and the Access Point MAC address listed in the Designated Root column.

4 Click the *Logout* button to securely exit the Access Point applet. There will be a prompt confirming logout before the applet is closed.

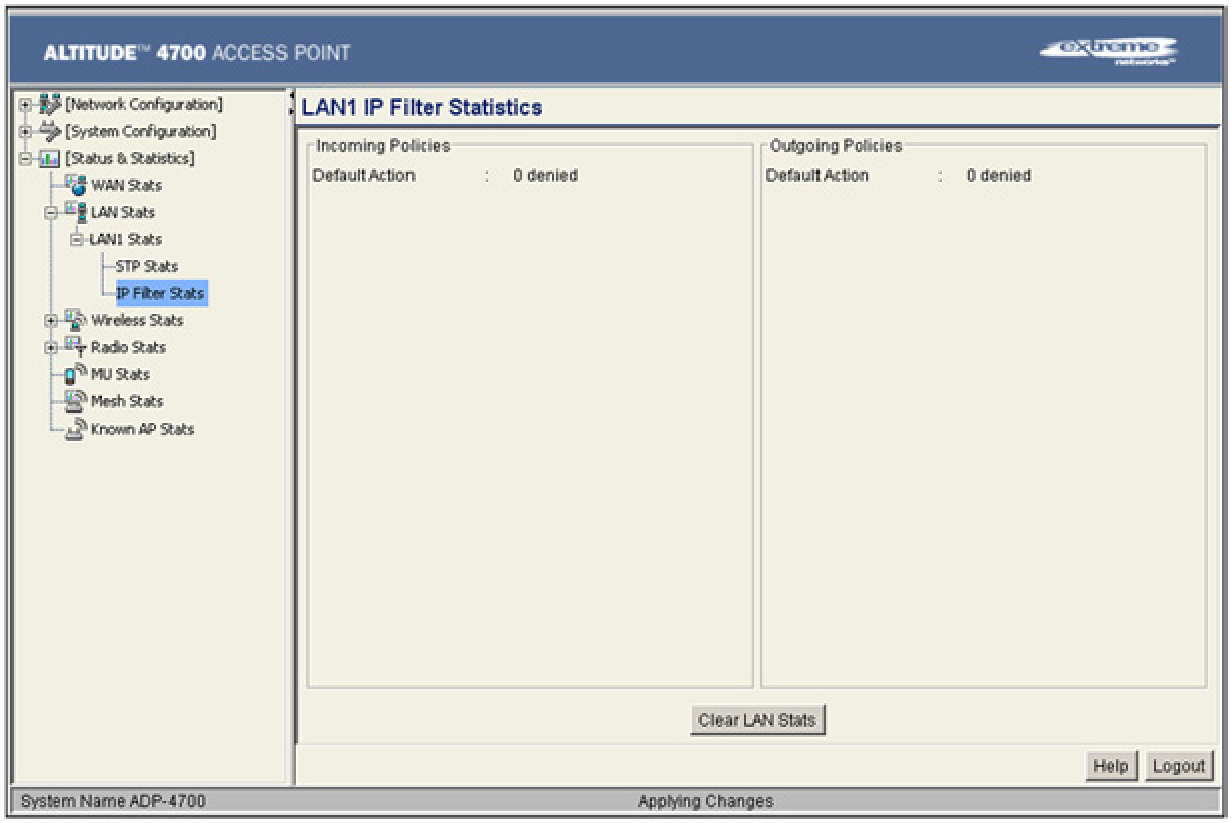
Viewing a LAN's IP Filter Statistics

Each Access Point LAN has the ability to track its own unique IP filter statistics. Refer to the LAN IP Filter Stats page to review statistics generated from both incoming and outgoing IP filtering policies. The LAN IP Filter Statistics screen shows a running count of packet traffic either allowed or denied when filter rules fail. These rules determine which IP packets are processed normally by LANs 1 and 2 and which are discarded.

For more information on how IP Filtering works and how its configured on the Access Point, see "Configuring IP Filtering" on page 188.

To view access point LAN's IP filter statistics:

1 Select *Status and Statistics* > *LAN Stats* > *LAN1 Stats* (or LAN2 Stats) > *IP Filter Stats* from the access point menu tree.



LAN1 IP Filter Statistics

Incoming Policies

Default Action : 0 denied

Outgoing Policies

Default Action : 0 denied

System Name ADP-4700 Applying Changes

2 Refer to the *Incoming Policies* field to assess the number of packets either allowed or denied access by the Access Point's filtering rules. These are packets that are incoming to the Access Point LAN.

3 Refer to the *Outgoing Policies* field to assess the number of packets either allowed or denied access by the Access Point's filtering rules. These are packets that are outgoing from the Access Point LAN.

4 Click the *Clear LAN Stats* button to reset each of the data collection counters to zero in order to begin new data collections.

5 Click the *Logout* button to securely exit the Access Point applet. There will be a prompt confirming logout before the applet is closed.

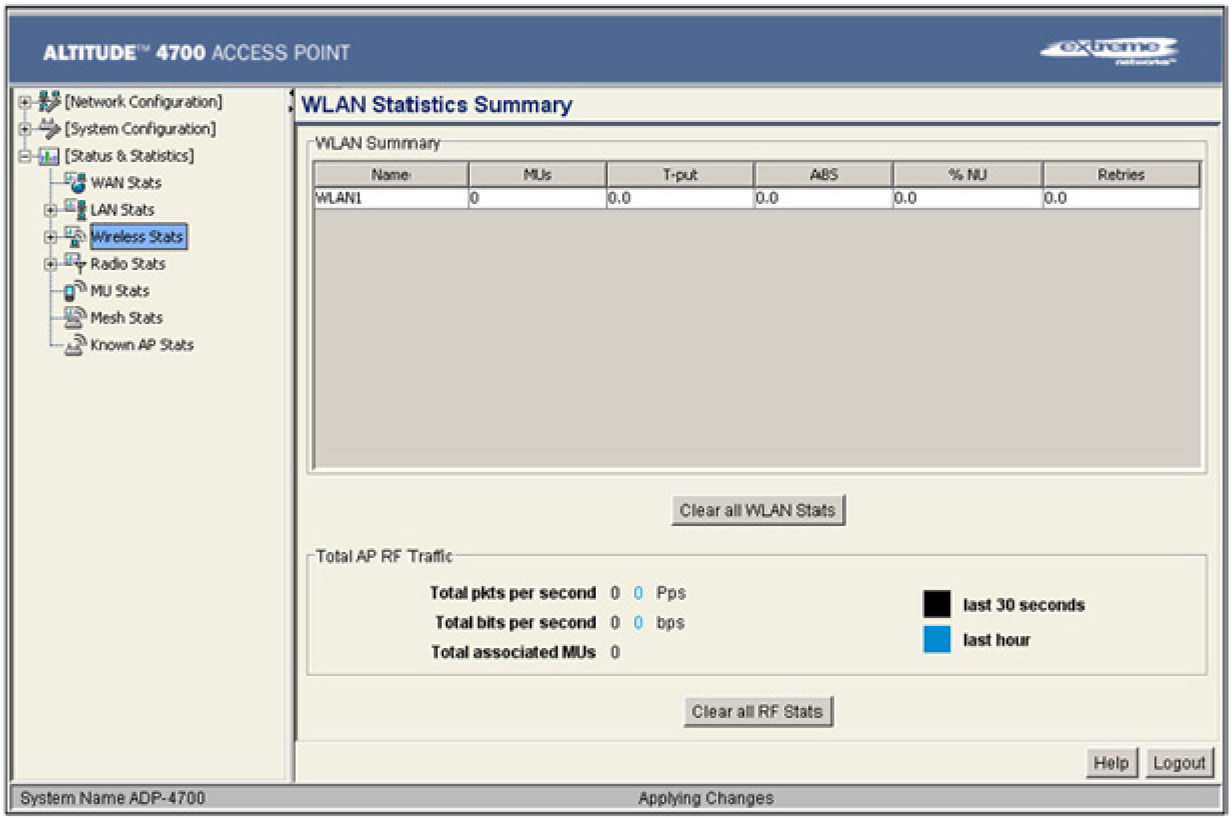
Viewing Wireless Statistics

Use the *WLAN Statistics Summary* screen to view overview statistics for active (enabled) WLANs on the access point. The *WLAN Summary* field displays basic information such as number of Mobile Units (MUs) and total throughput for each of the active WLANs. The *Total RF Traffic* section displays basic throughput information for all RF activity on the access point. The WLAN Statistics Summary screen is view-only with no user configurable data fields.

If a WLAN is not displayed within the *Wireless Statistics Summary* screen, see "Enabling Wireless LANs (WLANs)" on page 146 to enable the WLAN. For information on configuring the properties of individual WLANs, see "Creating/Editing Individual WLANs" on page 148.

To view access point WLAN Statistics:

1 Select *Status and Statistics* > *Wireless Stats* from the access point menu tree.



WLAN Statistics Summary

WLAN Summary

Name	MUs	T-put	ABS	% NU	Retries
WLAN1	0	0.0	0.0	0.0	0.0

Total AP RF Traffic

Total pkts per second 0 0 Pps
Total bits per second 0 0 bps
Total associated MUs 0

■ last 30 seconds
🟦 last hour

System Name ADP-4700 Applying Changes

2 Refer to the *WLAN Summary* field to reference high-level data for each enabled WLAN.

Name
Displays the names of all the enabled WLANs on the access point.

MUs
Displays the total number of MUs currently associated with each enabled WLAN. Use this information to assess if the MUs are properly grouped by function within each enabled WLAN.

T-put
Displays the total throughput in Megabits per second (Mbps) for each active WLAN.

ABS
Displays the *Average Bit Speed (ABS)* in Megabits per second (Mbps) for each active WLAN displayed.

% NU
Displays a percentage of the total packets for each active WLAN that are non-unicast. Non-unicast packets include broadcast and multicast packets.

Retries
Displays the average number of retries per packet. An excessive number could indicate possible network or hardware problems.

Clear All WLAN Stats
Click this button to reset each of the data collection counters to zero in order to begin new data collections.

Do not clear the WLAN stats if currently in an important data gathering activity or risk losing all data calculations to that point.

3 Refer to the *Total AP RF Traffic* field to view throughput information for the access point and WLAN.

Total pkts per second
Displays the average number of RF packets sent per second across all active WLANs on the access point. The number in black represents packets for the last 30 seconds and the number in blue represents total pkts per second for the last hour.

Total bits per second
Displays the average bits sent per second across all active WLANs on the Access Point. The number in black displays this statistic for the last 30 seconds and the number in blue displays this statistic for the last hour.

Total associated MUs
Displays the current number of MUs associated with the active WLANs on the access point. If the number is excessive, reduce the maximum number of MUs that can associate with the access point.

Clear all RF Stats
Click the *Clear all RF Stats* button to reset statistic counters for each WLAN, and the Total AP RF totals to 0. Do not clear RF stats if currently in an important data gathering activity or risk losing all data calculations to that point.

4 Click the *Clear RF Stats* button to reset each of the data collection counters to zero in order to begin new data collections.

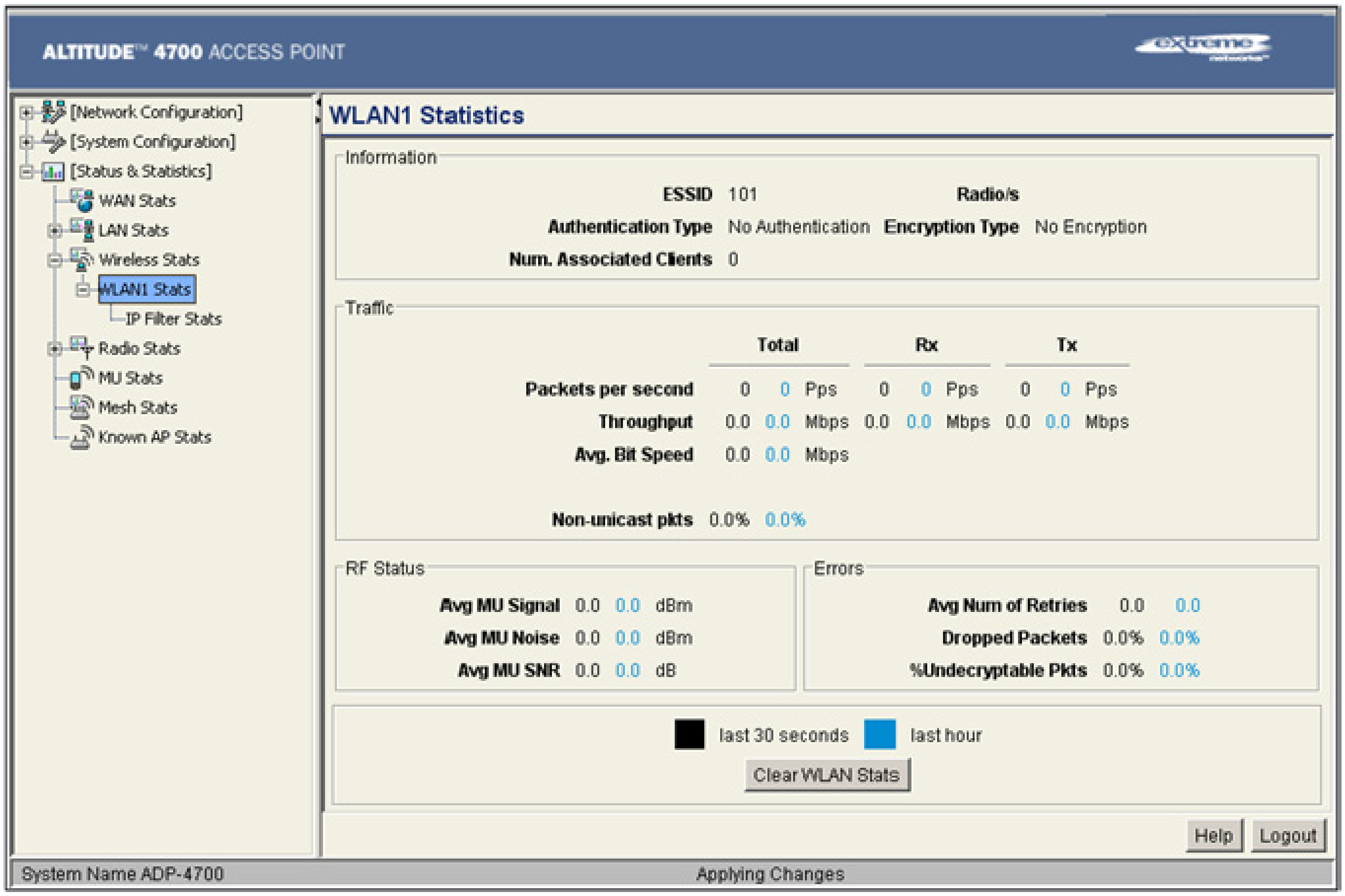
5 Click the *Logout* button to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Viewing WLAN Statistics

Use the *WLAN Stats* screen to view detailed statistics for individual WLANs.The WLAN Stats screen is separated into four fields; *Information*, *Traffic*, *RF Status*, and *Errors*. The *Information* field displays basic information such as number of associated Mobile Units, ESSID and security information. The *Traffic* field displays statistics on RF traffic and throughput. The *RF Status* field displays information on RF signal averages from the associated MUs. The *Error* field displays RF traffic errors based on retries, dropped packets, and undecryptable packets. The *WLAN Stats* screen is view-only with no user configurable data fields.

To view statistics for an individual WLAN:

1 Select *Status and Statistics* > *Wireless Stats* > *WLANx Stats* (*x* = target WLAN) from the access point menu tree.



WLAN1 Statistics

Information

ESSID 101 Radio/s

Authentication Type No Authentication Encryption Type No Encryption

Num. Associated Clients 0

Traffic

	Total			Rx			Tx		
Packets per second	0	0	Pps	0	0	Pps	0	0	Pps
Throughput	0.0	0.0	Mbps	0.0	0.0	Mbps	0.0	0.0	Mbps
Avg. Bit Speed	0.0	0.0	Mbps						
Non-unicast pkts	0.0%	0.0%							

RF Status

Avg MU Signal	0.0	0.0	dBm
Avg MU Noise	0.0	0.0	dBm
Avg MU SNR	0.0	0.0	dB

Errors

Avg Num of Retries	0.0	0.0
Dropped Packets	0.0%	0.0%
%Undecryptable Pkts	0.0%	0.0%

■ last 30 seconds 🟦 last hour

System Name ADP-4700 Applying Changes

2 Refer to the *Information* field to view specific WLAN address, MU and security scheme information for the WLAN selected from the access point menu tree.

ESSID	Displays the *Extended Service Set ID (ESSID)* for the target WLAN.
Radio/s	Displays the name of the 802.11a/n or 802.11b/g/n radio the target WLAN is using for access point transmissions.
Authentication Type	Displays the authentication type (802.1x EAP or Kerberos) defined for the WLAN. If the authentication type does not match the desired scheme for the WLAN or needs to be enabled.
Encryption Type	Displays the encryption method defined for the WLAN. If the encryption type does not match the desired scheme for the WLAN or needs to be enabled.
Num. Associated MUs	Displays the total number of MUs currently associated with the WLAN. If this number seems excessive, consider segregating MU's to other WLANs if appropriate.

3 Refer to the *Traffic* field to view performance and throughput information for the WLAN selected from the access point menu tree.

Pkts per second	The *Total* column displays the average total packets per second crossing the selected WLAN. The *Rx* column displays the average total packets per second received on the selected WLAN. The *Tx* column displays the average total packets per second sent on the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
Throughput	The *Total* column displays average throughput in Mbps for a given time period on the selected WLAN. The *Rx* column displays average throughput in Mbps for packets received on the selected WLAN. The *Tx* column displays average throughput for packets sent on the selected WLAN. The number in black represents statistics for the last 30 seconds and the number in blue represents statistics for the last hour. Use this information to assess whether the current access point data rate is sufficient to support required network traffic.
Avg. Bit Speed	The *Total* column displays the average bit speed in Mbps for a given time period on the selected WLAN.This includes all packets that are sent and received. The number in black represents statistics for the last 30 seconds and the number in blue represents statistics for the last hour. If the bit speed is significantly slower than the selected data rate, refer to the *RF Statistics* and *Errors* fields to troubleshoot.
% Non-unicast pkts	Displays the percentage of the total packets that are non-unicast. Non-unicast packets include broadcast and multicast packets.The number in black represents packets for the last 30 seconds and the number in blue represents packets for the last hour.

4 Refer to the *RF Status* field to view the following MU signal, noise and performance information for the WLAN selected from the access point menu tree.

Avg MU Signal	Displays the average RF signal strength in dBm for all MUs associated with the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour. If the signal is low, consider mapping the MU to a different WLAN if a better functional grouping of MUs can be determined.
Avg MU Noise	Displays the average RF noise for all MUs associated with the selected WLAN. The number in black represents MU noise for the last 30 seconds and the number in blue represents MU noise for the last hour. If MU noise is excessive, consider moving the MU closer to the access point, or in area with less conflicting network traffic.
Avg MU SNR	Displays the average *Signal to Noise Ratio (SNR)* for all MUs associated with the selected WLAN. The Signal to Noise Ratio is an indication of overall RF performance on your wireless networks.

5 Refer to the *Errors* field to view MU association error statistics for the WLAN selected from the access point menu tree.

Avg Num of Retries Displays the average number of retries for all MUs associated with the selected WLAN. The number in black represents average retries for the last 30 seconds and the number in blue represents average retries for the last hour.

Dropped Packets Displays the percentage of packets which the AP gave up on for all MUs associated with the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

% of Undecryptable Pkts Displays the percentage of undecryptable packets for all MUs associated with the selected WLAN. The number in black represents undecryptable pkts for the last 30 seconds and the number in blue represents undecryptable pkts for the last hour.

NOTE

The Apply and Undo Changes buttons are not available on the WLAN Statistics screen as this screen is view only with no configurable data fields.

6 Click the *Clear WLAN Stats* button to reset each of the data collection counters to zero in order to begin new data collections.

Do not clear the WLAN stats if currently in an important data gathering activity or risk losing all data calculations to that point.

7 Click the *Logout* button to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

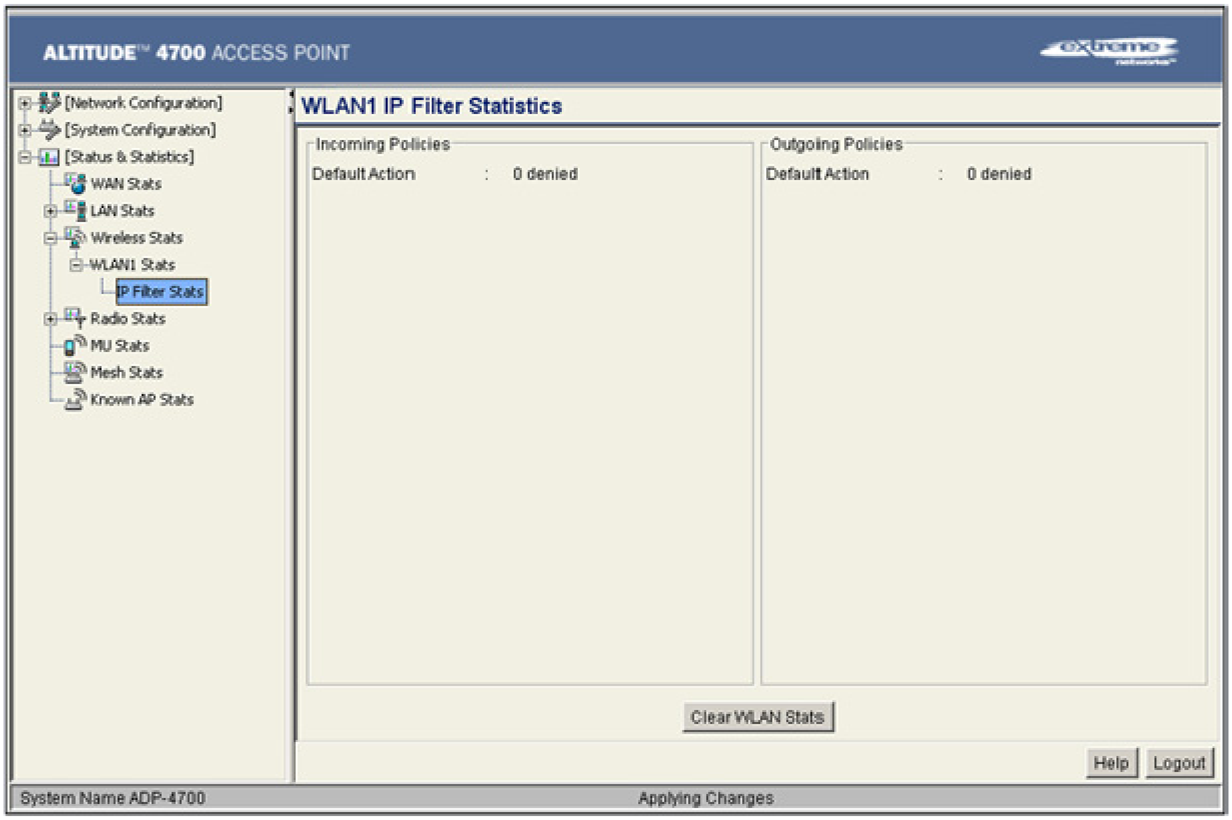
Viewing a WLAN’s IP Filter Statistics

Each Access Point WLAN has the ability to track its own unique IP filter statistics. Refer to the WLAN IP Filter Stats page to review statistics generated from both incoming and outgoing IP filtering policies supporting impacting the WLAN. The LAN IP Filter Statistics screen shows a running count of packet traffic either allowed or denied when filter rules fail. These rules determine which IP packets are processed normally by the selected WLAN and which are discarded.

For more information on how IP Filtering works and how its configured on the Access Point, see “Configuring IP Filtering” on page 188.

To view access point LAN's IP filter statistics:

1 Select *Status and Statistics* > *Wireless Stats* > *WLAN1 Stats* (or any other WLAN) > *IP Filter Stats* from the access point menu tree.



WLAN1 IP Filter Statistics

Incoming Policies
Default Action : 0 denied

Outgoing Policies
Default Action : 0 denied

System Name ADP-4700
Applying Changes

2 Refer to the *Incoming Policies* field to assess the number of packets either allowed or denied access by the Access Point's filtering rules. These are packets that are incoming to the selected Access Point WLAN.

3 Refer to the *Outgoing Policies* field to assess the number of packets either allowed or denied access by the Access Point's filtering rules. These are packets that are outgoing from the selected Access Point WLAN.

4 Click the *Clear LAN Stats* button to reset each of the data collection counters to zero in order to begin new data collections.

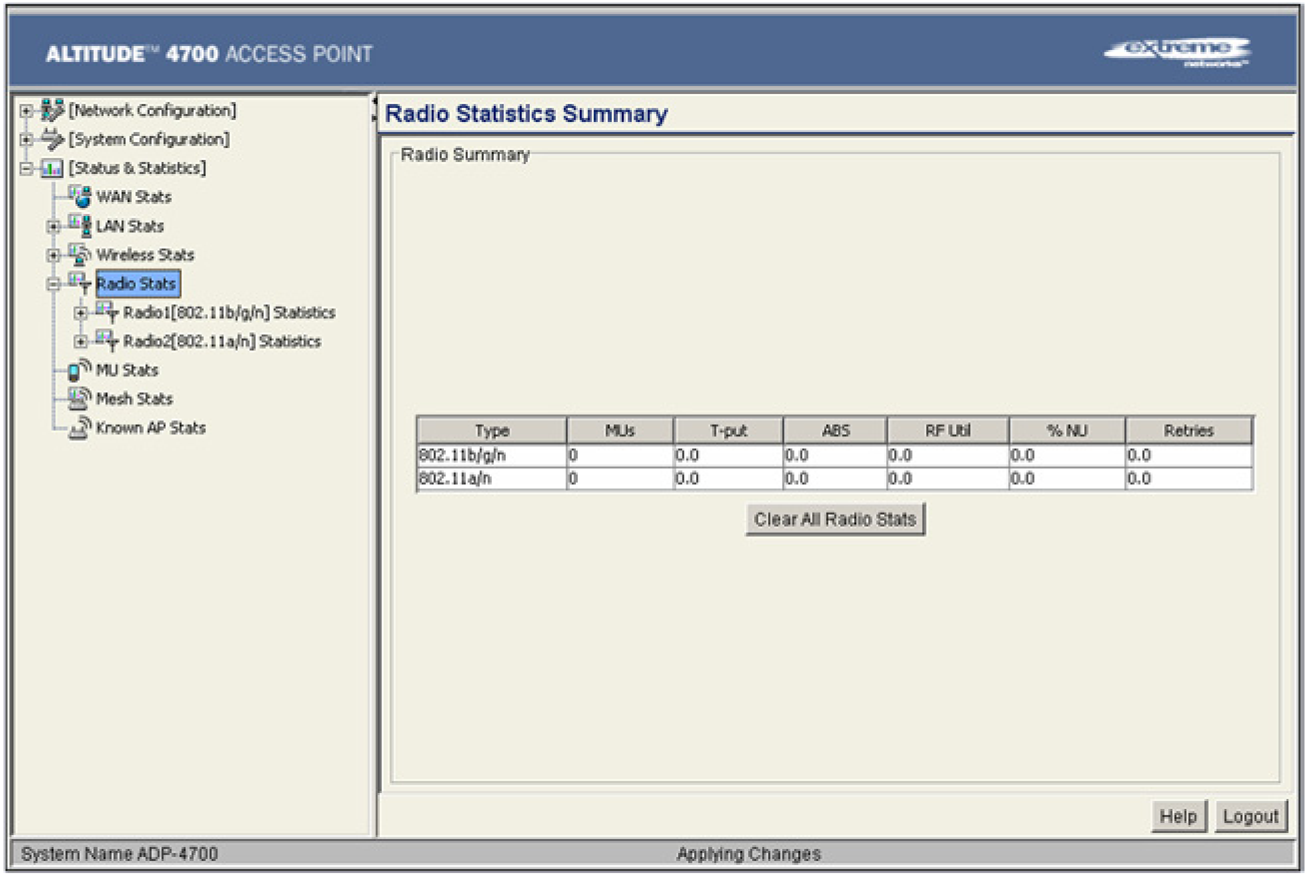
5 Click the *Logout* button to securely exit the Access Point applet. There will be a prompt confirming logout before the applet is closed.

Viewing Radio Statistics Summary

Select the *Radio Stats Summary* screen to view high-level information (radio name, type, number of associated MUs, etc.) for the radio(s) enabled on an access point. Individual radio statistics can be displayed as well by selecting a specific radio from within the access point menu tree.

To view high-level access point radio statistics:

1 Select *Status and Statistics* > *Radio Stats* from the access point menu tree.



Radio Statistics Summary

Radio Summary

Type	MUs	T-put	ABS	RF Util	% NU	Retries
802.11b/g/n	0	0.0	0.0	0.0	0.0	0.0
802.11a/n	0	0.0	0.0	0.0	0.0	0.0

2 Refer to the *Radio Summary* field to reference access point radio information.

Type — Displays the type of radio (either 802.11a/n or 802.11b/g/n) currently deployed by the access point.

MUs — Displays the total number of MUs currently associated with each access point radio.

T-put — Displays the total throughput in Megabits per second (Mbps) for each access point radio listed.

ABS — Displays the *Average Bit Speed (ABS)* in Megabits per second (Mbps) for each access point radio.

RF Util — Displays the approximate RF Utilization for each access point radio

% NU — Displays the percentage of the total packets that are non-unicast. Non-unicast packets include broadcast and multicast packets.

Retries — Displays the average number of retries per packet on each radio. A high number could indicate network or hardware problems.

3 Click the *Clear All Radio Stats* button to reset each of the data collection counters to zero in order to begin new data collections.

Do not clear the radio stats if currently in an important data gathering activity or risk losing all data calculations to that point.

For information on viewing radio statistics particular to the access point radio type displayed within the AP Stats Summary screen, see "Viewing Radio Statistics" on page 278.

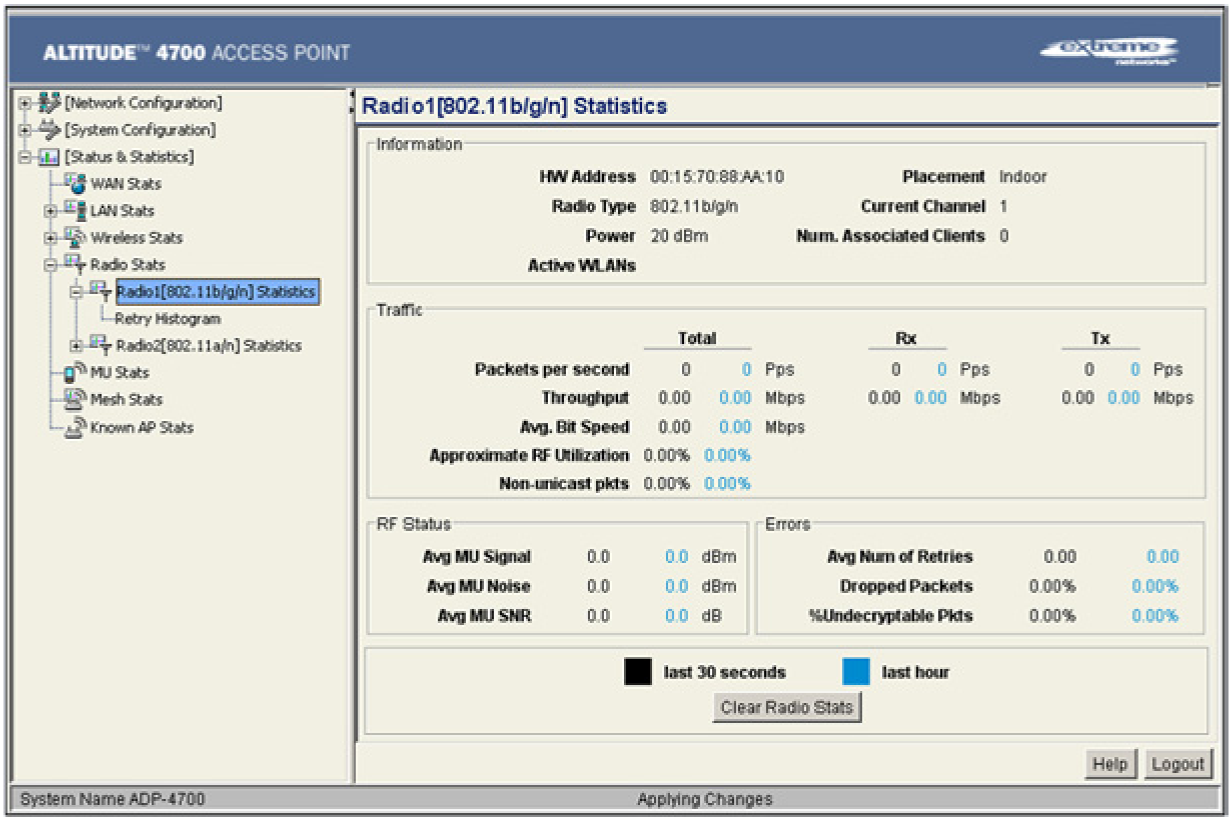
4 Click the *Logout* button to securely exit the Access Point applet.

Viewing Radio Statistics

Refer to the *Radio Stats* screen to view detailed information for the access point radio (either 802.11a/n or 802.11b/g/n) displayed within the Radio Summary screen. There are four fields within the screen. The *Information* field displays device address and location information, as well as channel and power information. The *Traffic* field displays statistics for cumulative packets, bytes, and errors received and transmitted. The Traffic field does not add retry information to the stats displayed. Refer to the *RF Status* field for an average MU signal, noise and signal to noise ratio information. Finally, the *Errors* field displays retry information as well as data transmissions the access point radio either dropped or could not decrypt. The information within the 802.11a/n Radio Statistics screen is view-only with no configurable data fields.

To view detailed radio statistics:

1 Select *Status and Statistics > Radio Stats > Radio1(802.11b/g/n) Stats* from the access point menu tree.



Radio1[802.11b/g/n] Statistics

Information

HW Address	00:15:70:88:AA:10	Placement	Indoor
Radio Type	802.11b/g/n	Current Channel	1
Power	20 dBm	Num. Associated Clients	0
Active WLANs			

Traffic

	Total			Rx			Tx		
Packets per second	0	0	Pps	0	0	Pps	0	0	Pps
Throughput	0.00	0.00	Mbps	0.00	0.00	Mbps	0.00	0.00	Mbps
Avg. Bit Speed	0.00	0.00	Mbps						
Approximate RF Utilization	0.00%	0.00%							
Non-unicast pkts	0.00%	0.00%							

RF Status

Avg MU Signal	0.0	0.0	dBm
Avg MU Noise	0.0	0.0	dBm
Avg MU SNR	0.0	0.0	dB

Errors

Avg Num of Retries	0.00	0.00
Dropped Packets	0.00%	0.00%
%Undecryptable Pkts	0.00%	0.00%

■ last 30 seconds 🟦 last hour

System Name ADP-4700 Applying Changes

2 Refer to the *Information* field to view the access point 802.11a/n or 802.11b/g/n radio's MAC address, placement and transmission information.

HW Address

The *Media Access Control (MAC)* address of the access point housing the 802.11a/n radio. The MAC address is set at the factory and can be found on the bottom of the Access Point.

Radio Type

Displays the radio type (either 802.11a/n or 802.11b/g/n).

Power

The power level in milliwatts (mW) for RF signal strength.

Active WLANs

Lists the access point WLANs adopted by the 802.11a/n or 802.11b/g/n radio.

Placement

Lists whether the access point radio is indoors or outdoors.

Current Channel

Indicates the channel for communications between the access point radio and its associated MUs.

Num Associated MUs

Lists the number of mobile units (MUs) currently associated with the access point 802.11a/n or 802.11b/g/n radio.

3 Refer to the *Traffic* field to view performance and throughput information for the target access point 802.11a/n or 802.11b/g/n radio.

Pkts per second

The *Total* column displays the average total packets per second crossing the radio. The *Rx* column displays the average total packets per second received. The *Tx* column displays the average total packets per second transmitted. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

Throughput

The *Total* column displays average throughput on the radio. The *Rx* column displays average throughput in Mbps for packets received. The *Tx* column displays average throughput for packets transmitted. The number in black represents statistics for the last 30 seconds and the number in blue represents statistics for the last hour. Use this information to assess whether the current throughput is sufficient to support required network traffic.

Avg. Bit Speed

The *Total* column displays the average bit speed in Mbps for the radio This includes all packets transmitted and received. The number in black represents statistics for the last 30 seconds and the number in blue represents statistics for the last hour.

Approximate RF Utilization

The approximate RF utilization of the access point radio. This value is calculated as throughput divided by average bit speed. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

% Non-unicast pkts

Displays the percentage of total radio packets that are non-unicast. Non-unicast packets include broadcast and multicast packets.The number in black represents packets for the last 30 seconds and the number in blue represents packets for the last hour.

4 Refer to the *RF Status* field to view the following MU signal, noise and performance information for the target access point 802.11a/n or 802.11b/g/n radio.

Avg MU Signal	Displays the average RF signal strength in dBm for all MUs associated with the radio. The number in black represents the average signal for the last 30 seconds and the number in blue represents the average signal for the last hour. If the signal is low, consider mapping the MU to a different WLAN, if a better functional grouping of MUs can be determined.
Avg MU Noise	Displays the average RF noise for all MUs associated with the access point radio. The number in black represents MU noise for the last 30 seconds and the number in blue represents MU noise for the last hour. If MU noise is excessive, consider moving the MU closer to the access point, or in area with less conflicting network traffic.
Avg MU SNR	Displays the average *Signal to Noise Ratio (SNR)* for all MUs associated with the access point radio. The Signal to Noise Ratio is an indication of overall RF performance on your wireless network.

5 Refer to the *Errors* field to reference retry information as well as data transmissions the target access point 802.11a/n or 802.11 b/g radio either gave up on could not decrypt.

Avg Num. of Retries	Displays the average number of retries for all MUs associated with the access point 802.11a/n or 802.11b/g/n radio. The number in black represents retries for the last 30 seconds and the number in blue represents retries for the last hour.
Dropped Packets	Displays the percentage of packets the AP gave up on for all MUs associated with the access point 802.11a/n or 802.11b/g/n radio. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
% of Undecryptable Pkts	Displays the percentage of undecryptable packets for all MUs associated with the 802.11a/n or 802.11b/g/n radio. The number in black represents packets for the last 30 seconds and the number in blue represents packets for the last hour.

6 Click the *Clear Radio Stats* button to reset each of the data collection counters to zero in order to begin new data collections.

7 Click the *Logout* button to securely exit the Access Point applet.

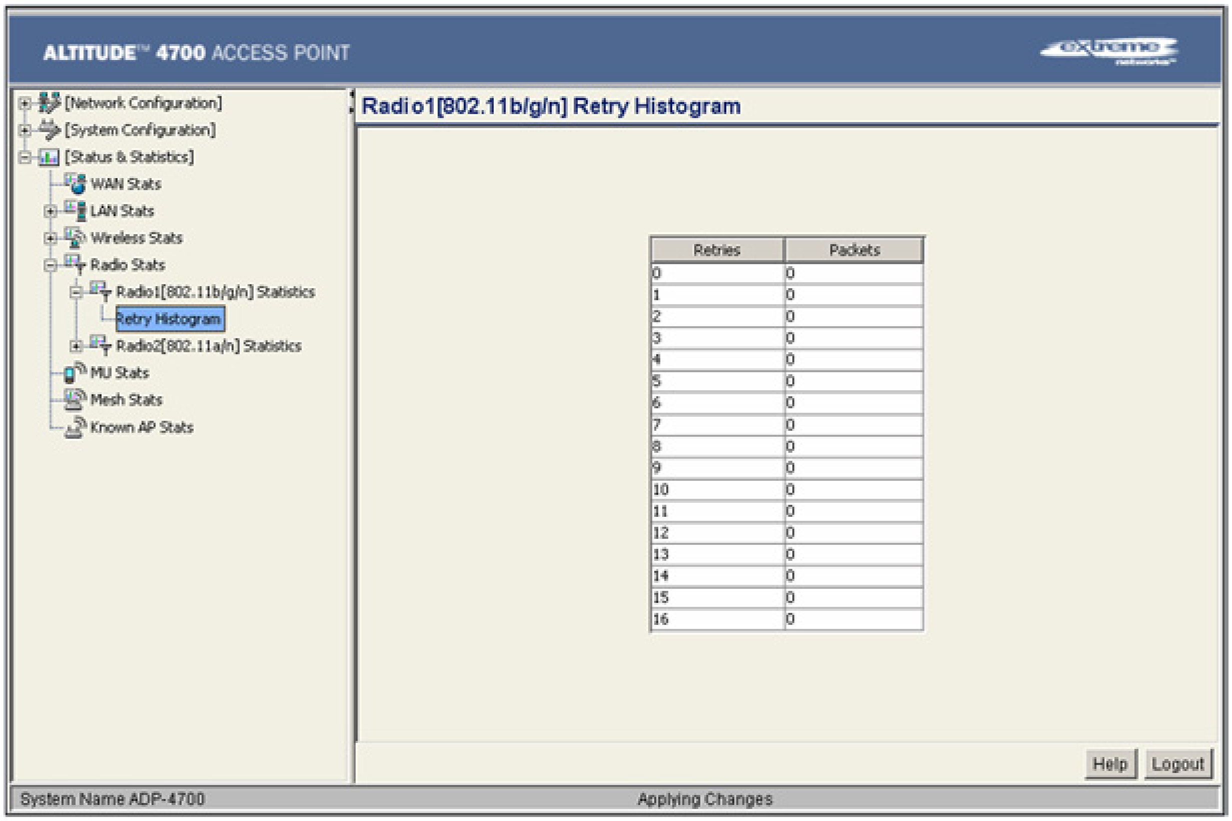
Retry Histogram

Refer to the *Retry Histogram* screen for an overview of the retries transmitted by an Access Point radio and whether those retries contained any data packets. Use this information in combination with the error fields within a Radio Stats screen to assess overall radio performance.

To display a Retry Histogram screen for an Access Point radio:

1 Select *Status and Statistics* > *Radio Stats* > *Radio1(802.11b/g/n) Stats* > *Retry Histogram* from the access point menu tree.

A Radio Histogram screen is available for each Access Point radio.



Retries	Packets
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0

The table's first column shows 0 under *Retries*. The value under the *Packets* column directly to the right shows the number of packets transmitted by this Access Point radio that required 0 retries (delivered on the first attempt). As you go down the table you can see the number of packets requiring 1 retry, 2 retries etc. Use this information to assess whether an abundance of retries warrants reconfiguring the Access Point radio to achieve better performance.

2 Click *Apply* to save any changes to the Radio Histogram screen. Navigating away from the screen without clicking Apply results in changes to the screens being lost.

3 Click *Undo Changes* (if necessary) to undo any changes made to the screen. Undo Changes reverts the settings to the last saved configuration.

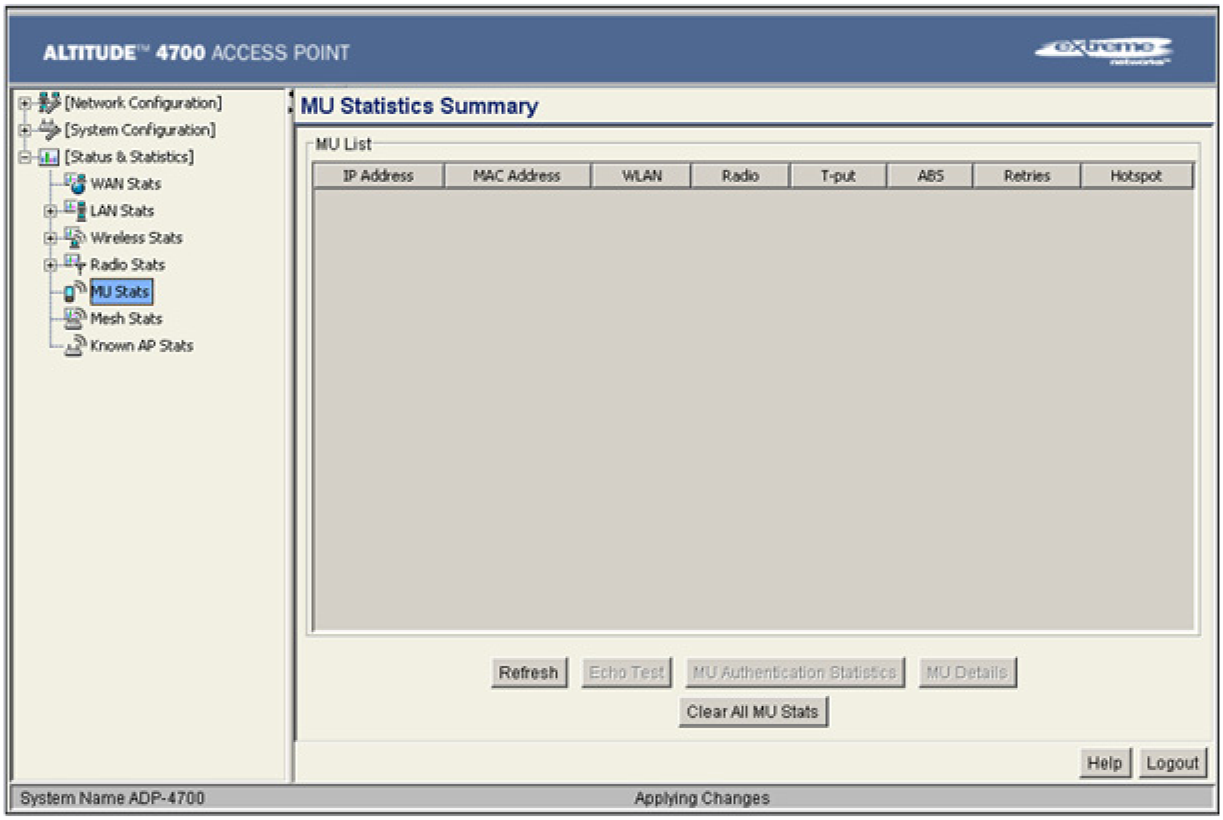
4 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Viewing MU Statistics Summary

Use the *MU Stats Summary* screen to display overview statistics for mobile units (MUs) associated with the access point. The *MU List* field displays basic information such as IP Address and total throughput for each associated MU. The MU Stats screen is view-only with no user configurable data fields. However, individual MUs can be selected from within the MU Stats Summary screen to either ping to assess interoperability or display authentication statistics.

To view access point overview statistics for all of the MUs associated to the access point:

1 Select *Status and Statistics* > *MU Stats* from the access point menu tree.



2 Refer to the *MU List* field to reference associated MU address, throughput and retry information.

IP Address Displays the IP address of each of the associated MU.

MAC Address Displays the MAC address of each of the associated MU.

WLAN Displays the WLAN name each MU is interoperating with.

Radio Displays the name of the 802.11a/n or 802.11b/g/n radio each MU is associated with.

T-put Displays the total throughput in Megabits per second (Mbps) for each associated MU.

ABS Displays the *Average Bit Speed (ABS)* in Megabits per second (Mbps) for each associated MU.

Retries Displays the average number of retries per packet. A high number retries could indicate possible network or hardware problems.

Hotspot Displays whether this radio is currently supporting a hotspot.

3 Click the *Refresh* button to update the data collections displayed without resetting the data collections to zero.

4 Click the *Echo Test* button to display a screen for verifying the link with an associated MU.

For detailed information on conducting a ping test for an MUs, see "Pinging Individual MUs" on page 285.

NOTE

An echo test initiated from the access point MU Stats Summary screen uses WNMP pings. Therefore, target clients that are not Motorola MUs are unable to respond to the echo test.

5 Click the *MU Authentication Statistics* button to display a screen with detailed authentication statistics for the an MU.

For information on individual MU authentication statistics, see "MU Authentication Statistics" on page 285.

6 Click the *MU Details* button to display a screen with detailed statistics for a selected MU.

For detailed information on individual MU authentication statistics, see "Viewing MU Details" on page 283.

7 Click the *Clear All MU Stats* button to reset each of the data collection counters to zero in order to begin new data collections.

8 Click the *Logout* button to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Viewing MU Details

Use the *MU Details* screen to display throughput, signal strength and transmit error information for a specific MU associated with the access point.

The MU Details screen is separated into four fields; *MU Properties*, *MU Traffic*, *MU Signal*, and *MU Errors*. The *MU Properties* field displays basic information such as hardware address, IP address, and associated WLAN and AP. Reference the *MU Traffic* field for MU RF traffic and throughput data. Use the *RF Status* field to reference information on RF signal averages from the target MU. The *Error* field displays RF traffic errors based on retries, dropped packets and undecryptable packets. The MU Details screen is view-only with no user configurable data fields.

To view details specific to an individual MU:

1 Select *Status and Statistics* > *MU Stats* from the access point menu tree.

2 Highlight a specific MU.

3 Select the *MU Details* button.

4 Refer to the *MU Properties* field to view MU address information.

IP Address — Displays the IP address of the MU.

WLAN Association — Displays the name of the WLAN the MU is associated with. Use this information to assess whether the MU is properly grouped within that specific WLAN.

PSP State — Displays the current PSP state of the MU. The *PSP Mode* field has two potential settings. PSP indicates the MU is operating in Power Save Protocol mode. In PSP, the MU runs enough power to check for beacons and is otherwise inactive. CAM indicates the MU is continuously aware of all radio traffic. Extreme Networks recommends CAM for those MUs transmitting with the AP frequently and for periods of time of two hours.

HW Address — Displays the *Media Access Control (MAC)* address for the MU.

Radio Association

Displays the name of the AP MU is currently associated with.

QoS Client Type

Displays the data type transmitted by the mobile unit. Possible types include *Legacy*, *Voice*, *WMM Baseline* and *Power Save*.

Encryption

Displays the encryption scheme deployed by the associated MU.

5 Refer to the *Traffic* field to view individual MU RF throughput information.

Packets per second

The *Total* column displays average total packets per second crossing the MU. The *Rx* column displays the average total packets per second received on the MU. The *Tx* column displays the average total packets per second sent on the MU. The number in black represents Pkts per second for the last 30 seconds and the number in blue represents Pkts per second for the last hour.

Throughput

The *Total* column displays the average total packets per second crossing the selected MU. The *Rx* column displays the average total packets per second received on the MU. The *Tx* column displays the average total packets per second sent on the MU. The number in black represents throughput for the last 30 seconds, the number in blue represents throughput for the last hour.

Avg. Bit Speed

The *Total* column displays the average bit speed in Mbps for a given time period on the MU. This includes all packets sent and received. The number in black represents average bit speed for the last 30 seconds and the number in blue represents average bit speed for the last hour. Consider increasing the data rate of the AP if the current bit speed does not meet network requirements. The associated MU must also be set to the higher rate to interoperate with the access point at that data rate.

% of Non-unicast pkts

Displays the percentage of the total packets for the selected mobile unit that are non-unicast. Non-unicast packets include broadcast and multicast packets. The number in black represents packets for the last 30 seconds and the number in blue represents packets for the last hour.

6 Refer to the *RF Status* field to view MU signal and signal disturbance information.

Avg MU Signal

Displays RF signal strength in dBm for the target MU. The number in black represents signal information for the last 30 seconds and the number in blue represents signal information for the last hour.

Avg MU Noise

Displays RF noise for the target MU. The number in black represents noise for the last 30 seconds, the number in blue represents noise for the last hour.

Avg MU SNR

Displays the *Signal to Noise Ratio (SNR)* for the target MU. The Signal to Noise Ratio is an indication of overall RF performance on your wireless network.

7 Refer to the *Errors* field to view MU retry information and statistics on packets not transmitted.

Avg Num of Retries

Displays the average number of retries for the MU. The number in black represents average retries for the last 30 seconds and the number in blue represents average retries for the last hour.

Dropped Packets	Displays the percentage of packets the AP gave up as not received on for the selected MU. The number in black represents the percentage of packets for the last 30 seconds and the number in blue represents the percentage of packets for the last hour.
% of Undecryptable Pkts	Displays the percentage of undecryptable packets for the MU. The number in black represents the percentage of undecryptable packets for the last 30 seconds and the number in blue represents the percentage of undecryptable packets for the last hour.

8 Click *OK* to exit the screen.

Pinging Individual MUs

The access point can verify its link with an MU by sending WNMP ping packets to the associated MU. Use the *Echo Test* screen to specify a target MU and configure the parameters of the ping test.

NOTE

An echo test initiated from the access point MU Stats Summary screen uses WNMP pings. Therefore, target clients that are not Motorola MUs are unable to respond to the echo test.

To ping a specific MU to assess its connection with an access point:

1 Select *Status and Statistics* > *MU Stats* from the access point menu tree.

2 Select the *Echo Test* button from within the *MU Stats Summary* screen

3 Specify the following ping test parameters.

Station Address	The IP address of the target MU. Refer to the *MU Stats Summary* screen for associated MU IP address information.
Number of ping	Specify the number of ping packets to transmit to the target MU. The default is 100.
Packet Length	Specify the length of each data packet transmitted to the target MU during the ping test. The default is 100 bytes.
Packet Data	Defines the data to be transmitted as part of the test.

4 Click the *Ping* button to begin transmitting ping packets to the station address specified.

Refer to the *Number of Responses* parameter to assess the number of responses from the target MU versus the number of pings transmitted by the access point. Use the ratio of packets sent versus packets received to assess the link quality between MU and the access point

Click the *Ok* button to exit the Echo Test screen and return to the MU Stats Summary screen.

MU Authentication Statistics

The access point can access and display authentication statistics for individual MUs.

To view access point authentication statistics for a specific MU:

1 Select *Status and Statistics* > *MU Stats* from the access point menu tree.

2 Highlight a target MU from within the *MU List* field.

3 Click the *MU Authentication Statistics* button

Use the displayed statistics to determine if the target MU would be better served with a different access point WLAN or access point radio.

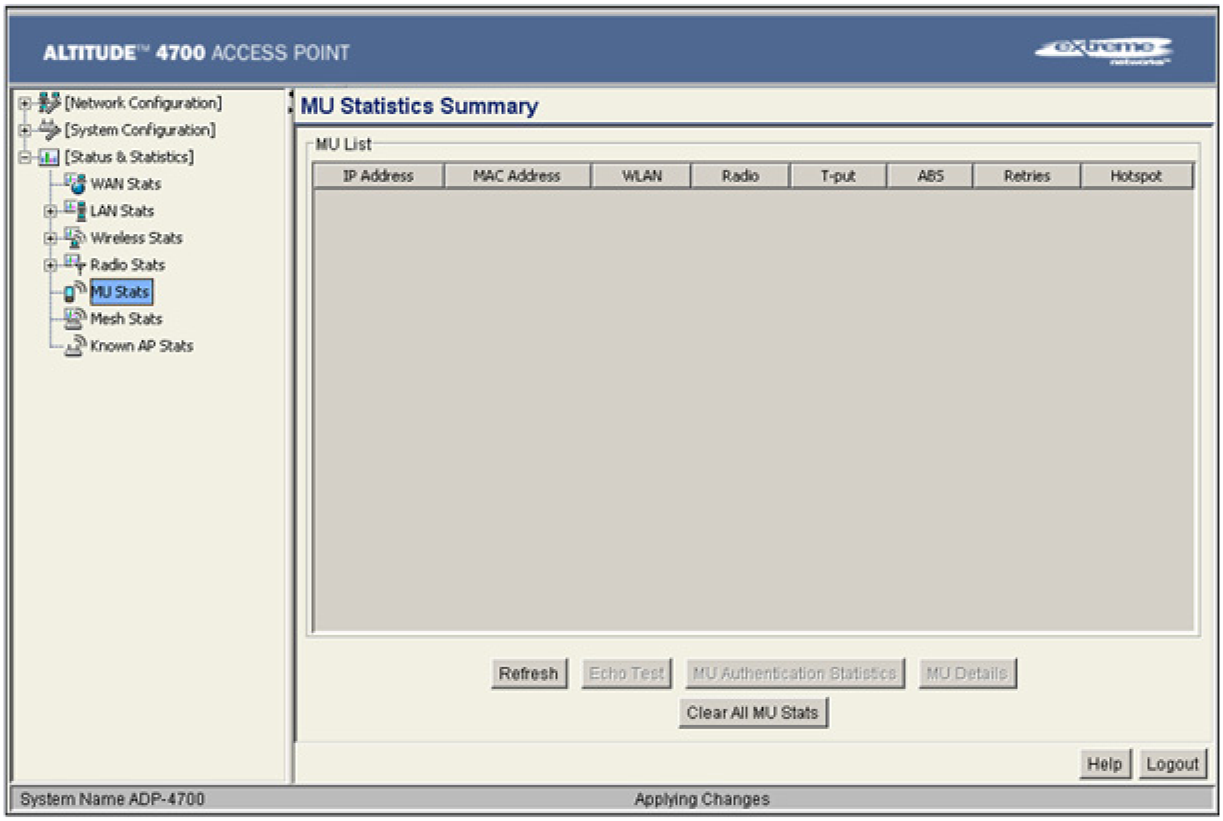
4 Click *Ok* to return to the MU Stats Summary screen.

Viewing the Mesh Statistics Summary

The access point has the capability of detecting and displaying the properties of other Access Points in mesh network (either base bridges or client bridges) mode. This information is used to create a list of known wireless bridges.

To view detected mesh network statistics:

1 Select *Status and Statistics* > *Mesh Stats* from the access point menu tree.



The *Mesh Statistics Summary* screen displays the following information:

Conn Type — Displays whether the bridge has been defined as a base bridge or a client bridge.

MAC Address

The unique 48-bit, hard-coded Media Access Control address, known as the devices station identifier. This value is hard coded at the factory by the manufacturer and cannot be changed.

WLAN

Displays the WLAN name each wireless bridge is interoperating with.

Radio

Displays the name of the 802.11a/n or 802.11b/g/n radio each bridge is associated with.

T-put

Displays the total throughput in Megabits per second (Mbps) for each associated bridge.

ABS

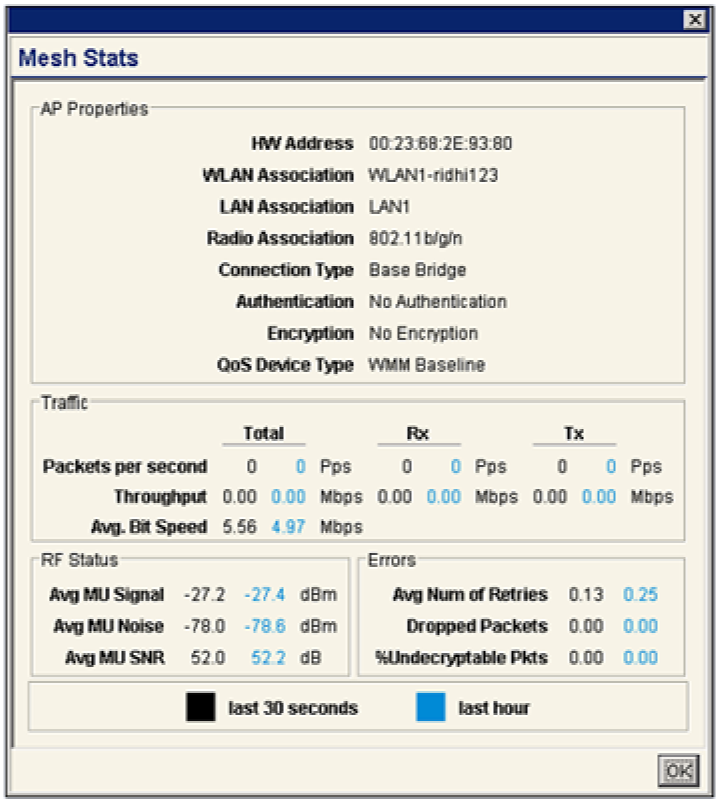
Displays the *Average Bit Speed (ABS)* in Megabits per second (Mbps) for each associated bridge.

Retries

Displays the average number of retries per packet. A high number retries could indicate possible network or hardware problems.

2 Click the *Refresh* button to update the display of the Mesh Statistics Summary screen to the latest values.

3 Click the *Details* button to display AP properties and radio information for those Access Points in a mesh configuration with this detecting Access Point.



Mesh Stats

AP Properties

HW Address	00:23:68:2E:93:80
WLAN Association	WLAN1-ridhi123
LAN Association	LAN1
Radio Association	802.11b/g/n
Connection Type	Base Bridge
Authentication	No Authentication
Encryption	No Encryption
QoS Device Type	WMM Baseline

Traffic

	Total			Rx			Tx		
Packets per second	0	0	Pps	0	0	Pps	0	0	Pps
Throughput	0.00	0.00	Mbps	0.00	0.00	Mbps	0.00	0.00	Mbps
Avg. Bit Speed	5.56	4.97	Mbps						

RF Status

Avg MU Signal	-27.2	-27.4	dBm
Avg MU Noise	-78.0	-78.6	dBm
Avg MU SNR	52.0	52.2	dB

Errors

Avg Num of Retries	0.13	0.25
Dropped Packets	0.00	0.00
%Undecryptable Pkts	0.00	0.00

■ last 30 seconds ■ last hour

4 Click the *Logout* button to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Viewing Known Access Point Statistics

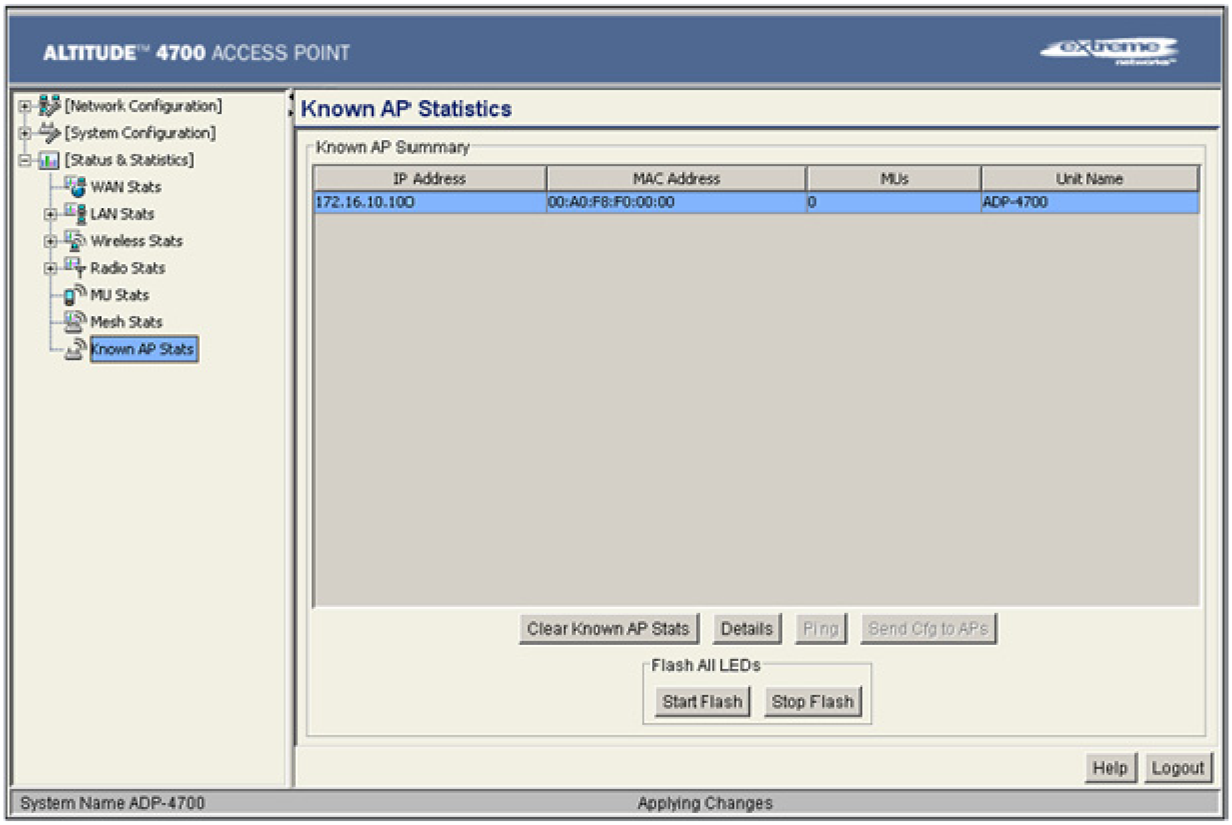
The access point has the capability of detecting and displaying the properties of other Extreme Networks Access Points located within its coverage area. Detected access point’s transmit a WNMP message indicating their channel, IP address, firmware version, etc. This information is used to create a known AP list. The list has field indicating the properties of the Access Point discovered.

NOTE

The Known AP Statistics screen only displays statistics for Access Points located on the same subnet.

To view detected Access Point statistics:

1 Select *Status and Statistics > Known AP Stats* from the access point menu tree.



Known AP Statistics

Known AP Summary

IP Address	MAC Address	MUs	Unit Name
172.16.10.100	00:A0:F8:F0:00:00	0	ADP-4700

System Name ADP-4700

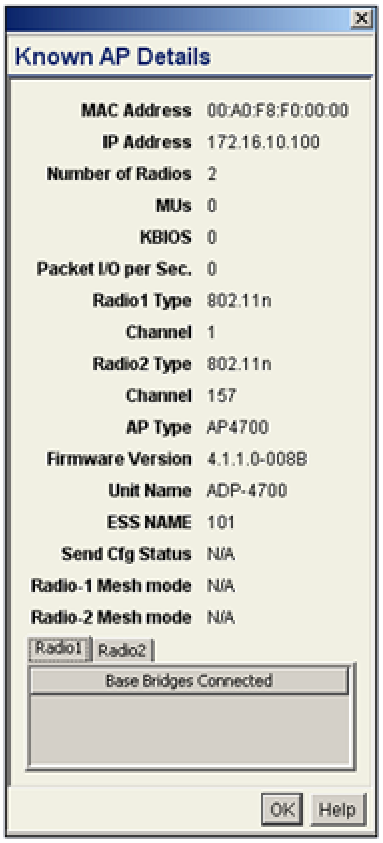
Applying Changes

The *Known AP Statistics* screen displays the following information:

IP Address	The network-assigned Internet Protocol address of the located AP.
MAC Address	The unique 48-bit, hard-coded Media Access Control address, known as the devices station identifier. This value is hard coded at the factory by the manufacturer and cannot be changed.
MUs	The number MUs associated with the located access point.
Unit Name	Displays the name assigned to the access point using the System Settings screen.

2 Click the *Clear Known AP Stats* button to reset each of the data collection counters to zero in order to begin new data collections.

3 Click the *Details* button to display Access Point address and radio information.



Known AP Details

MAC Address 00:A0:F8:F0:00:00
IP Address 172.16.10.100
Number of Radios 2
MUs 0
KBIOS 0
Packet I/O per Sec. 0
Radio1 Type 802.11n
Channel 1
Radio2 Type 802.11n
Channel 157
AP Type AP4700
Firmware Version 4.1.1.0-008B
Unit Name ADP-4700
ESS NAME 101
Send Cfg Status N/A
Radio-1 Mesh mode N/A
Radio-2 Mesh mode N/A

The Known AP Details screen displays the target AP’s MAC address, IP address, radio channel, number of associated MUs, packet throughput per second, radio type(s), model, firmware version, ESS and client bridges currently connected to the AP radio. Use this information to determine whether this AP provides better MU association support than the locating Access Point or warrants consideration as a member of a different mesh network.

4 Click the *Ping* button to display a screen for verifying the link with a highlighted Access Point.

NOTE

A ping test initiated from the access point Known AP Statistics screen uses WNMP pings. Therefore, target devices that are not Extreme Networks Access Points are unable to respond to the ping test.

5 Click the *Send Cfg to APs* button to send the your Access Point’s configuration to other Access Point’s. The recipient Access Point must be the same dual-radio model as the Access Point sending the configuration. The sending and recipient Access Point’s must also be running the same major firmware version.

CAUTION

When using the Send Cfg to APs function to migrate an Access Point’s configuration to other Access Points, it is important to keep in mind mesh network configuration parameters do not get completely sent to other Access Points. The Send Cfg to APs function will not send the “auto-select” and “preferred list” settings.

Additionally, LAN1 and LAN2 IP mode settings will only be sent if the sender's AP mode is DHCP or BOOTP. The WAN's IP mode will only be sent if the sender's IP mode is DHCP.

6 Click the *Start Flash* button to flash the LEDs of other access points detected and displayed within the Known AP Statistics screen.

   Use the *Start Flash* button to determine the location of the devices displayed within the Known AP Statistics screen. When an access point is highlighted and the Start Flash button is selected, the LEDs on the selected access point flash. When the *Stop Flash* button is selected, the LEDs on the selected access point go back to normal operation.

7 Click the *Logout* button to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

8

CHAPTER

CLI Reference

The access point *Command Line Interface (CLI)* is accessed through the serial port or a Telnet session. The access point CLI follows the same conventions as the Web-based user interface. The CLI does, however, provide an "escape sequence" to provide diagnostics for problem identification and resolution.

NOTE

The CLI commands described in this guide pertain equally to both the Altitude 4710 and Altitude 4750 Access Points.

The CLI treats the following as invalid characters:

```
<   >   |   "   &   \   ?   ,
```

In order to avoid problems when using the CLI, these characters should be avoided.

Connecting to the CLI

Accessing the CLI through the Serial Port

To connect to the access point CLI through the serial port:

1 Connect one end of a null modem serial cable to the access point's serial connector.

2 Attach the other end of the null modem serial cable to the serial port of a PC running HyperTerminal or a similar emulation program.

3 Set the HyperTerminal program to use 19200 baud, 8 data bits, 1 stop bit, no parity, no flow control, and auto-detect for terminal emulation.

4 Press <ESC> or <Enter> to enter into the CLI.

5 Enter the default username of *admin* and the default password of *admin123*. If this is your first time logging into the access point, you are unable to access any of the access point's commands until the country code is set. A new password will also need to be created.

Accessing the CLI via Telnet

To connect to the access point CLI through a Telnet connection:

1 If this is your first time connecting to your access point, keep in mind the access point uses a static IP WAN address (10.1.1.1). Additionally, the access point's LAN port is set as a DHCP client.

2 Enter the default username of *admin* and the default password of *admin123*. If this is your first time logging into the access point, you are unable to access any of the access point's commands until the country code is set. A new password will also need to be created.

Admin and Common Commands

AP4700>admin>

Displays admin configuration options. The items available under this command are shown below.

Syntax

help	Displays general user interface help.
passwd	Changes the admin password.
summary	Shows a system summary.
network	Goes to the network submenu
system	Goes to the system submenu.
stats	Goes to the stats submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin>help

Displays general CLI user interface help.

Syntax

help	Displays command line help using combinations of function keys for navigation.

Example

```
admin>help

  ?                           : display command help - Eg. ?, show ?, s?
* Restriction of “?”:         : “?” after a function argument is treated
                              : as an argument
                              : Eg. admin<network.lan> set lan enable?
                              : (Here “?” is an invalid extra argument,
                              : because it is after the argument
                              : “enable”)

  <ctrl-q>                    : go backwards in command history
  <ctrl-p>                    : go forwards in command history

  * Note                      : 1) commands can be incomplete
                              : - Eg. sh = sho = show
                              : 2) “//” introduces a comment and gets no
                              : resposne from CLI.

admin>
```

AP4700>admin>passwd

Changes the password for the admin login.

Syntax

passwd	Changes the admin password for access point access. This requires typing the old admin password and entering a new password and confirming it. Passwords can be up to 11 characters. The access point CLI treats the following as invalid characters: ' " \ & $ ^ * + ? [({ | , < > In order to avoid problems when using the access point CLI, these characters should be avoided.

Example

```
admin>passwd

Old Admin Password:******
New Admin Password (0 - 11 characters):******
Verify Admin Password (0 - 11 characters):******
```

For information on configuring passwords using the applet (GUI), see “Setting Passwords” on page 198.

AP4700>admin>summary

Displays the access point’s system summary.

Syntax

summary	Displays a summary of high-level characteristics and settings for the WAN, LAN and WLAN.

Example

```
admin>summary

AP4700 firmware version           : 4.1.1.0-022R
country code                      : us
ap-mode                           : independent
serial number                     : 10289-80867
model                             : AP4750-US
hw version                        : A

WLAN 1:
WLAN name                         : lobby
ESS ID                            : 101
Radio Band(s)                     : 5.0 GHz
VLAN                              : VLAN_1
Security Policy                   : Default
QoS Policy                        : Default
Rate Limiting                     : disabled

LAN1 Name: LAN1
LAN1 Mode: enable
LAN1 IP: 10.255.108.230
LAN1 Mask: 255.255.255.0
LAN1 DHCP Mode: client

LAN2 Name: LAN2
LAN2 Mode: enable
LAN2 IP: 192.168.1.1
LAN2 Mask: 255.255.255.0
LAN2 DHCP Mode: client

 WAN Interface  IP Address      Network Mask     Default Gateway  DHCP Client
 ------------------------------------------------------------------------------
    enable     0.0.0.0         255.0.0.0        0.0.0.0           disable
```

For information on displaying a system summary using the applet (GUI), see “Basic Device Configuration” on page 65.

AP4700>admin>..

Displays the parent menu of the current menu.

This command appears in all of the submenus under admin. In each case, it has the same function, to move up one level in the directory structure.

Example

```
admin(network.lan)>..
admin(network)>
```

AP4700>admin> /

Displays the root menu, that is, the top-level CLI menu.

This command appears in all of the submenus under admin. In each case, it has the same function, to move up to the top level in the directory structure.

Example

```
admin(network.lan)>/
admin>
```

AP4700>admin>save

Saves the configuration to system flash.

The save command appears in all of the submenus under admin. In each case, it has the same function, to save the current configuration.

Syntax

save	Saves configuration settings. The save command works at all levels of the CLI. The save command must be issued before leaving the CLI for updated settings to be retained.

Example

```
admin>save
admin>
```

AP4700>admin>quit

Exits the command line interface session and terminates the session.

The quit command appears in all of the submenus under admin. In each case, it has the same function, to exit out of the CLI. Once the quit command is executed, the login prompt displays again.

Example

```
admin>quit
```

Network Commands

AP4700>admin(network)>

Displays the network submenu. The items available under this command are shown below.

```
lan                             : go to LAN sub menu
wan                             : go to WAN sub menu
wireless                        : go to Wireless sub menu
firewall                        : go to Firewall sub menu
router                          : go to Router sub menu
ipfilter                        : go to IP Filtering sub menu
                                :
..                              : go to parent menu
/                               : go to root menu
                                :
save                            : save cfg to system flash
quit                            : quit cli
```

Network LAN Commands

AP4700>admin(network.lan)>

Displays the LAN submenu. The items available under this command are shown below.

show	Shows current access point LAN parameters.
set	Sets LAN parameters.
bridge	Goes to the mesh configuration submenu.
wlan-mapping	Goes to the WLAN/Lan/Vlan Mapping submenu.
dhcp	Goes to the LAN DHCP submenu.
type-filter	Goes to the Ethernet Type Filter submenu.
ipfpolicy	Goes to the LAN IP Filter Policy submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

For an overview of the LAN configuration options using the applet (GUI), see "Configuring the LAN Interface" on page 123.

AP4700>admin(network.lan)>show

Displays the access point LAN settings.

Syntax

show	Shows the settings for the access point LAN1 and LAN2 interfaces.

Example

```
admin(network.lan)>show

LAN On Ethernet Port                    : LAN1
LAN Ethernet Timeout                    : disable

802.1x Port Authentication:
      Username                          : admin
      Password                          : ********

Auto-negoitation                        : disable
Speed                                   : 100M
Duplex                                  : full

** LAN1 Information **
LAN Name                                : LAN1
LAN Interface                           : enable
802.11q Trunking                        : disable
Native VLAN Tag Mode                    : untagged

LAN IP mode                             : DHCP client
IP Address                              : 192.168.0.1
Network Mask                            : 255.255.255.255
Default Gateway                         : 192.168.0.1
Domain Name                             :
Primary DNS Server                      : 192.168.0.1
Secondary DNS Server                    : 192.168.0.2
WINS Server                             : 192.168.0.254

** LAN2 Information **
LAN Name                                : LAN2
LAN Interface                           : disable
802.11q Trunking                        : disable
Native VLAN Tag Mode                    : untagged

LAN IP mode                             : DHCP server
IP Address                              : 192.168.1.1
Network Mask                            : 255.255.255.255
Default Gateway                         : 192.168.1.1
Domain Name                             :
Primary DNS Server                      : 192.168.0.2
Secondary DNS Server                    : 192.168.0.3
WINS Server                             : 192.168.0.255
admin(network.lan)>
```

For information on displaying LAN information using the applet (GUI), see "Configuring the LAN Interface" on page 123.

AP4700>admin(network.lan)>set

Sets the LAN parameters for the LAN port.

Syntax

set	lan	<mode>	Enables or disables the access point LAN interface.
	name	<idx-name >	Defines the LAN name by index.
	ethernet-port-lan	<idx>	Defines which LAN (LAN1 or LAN2) is active on the Ethernet port.
	timeout	<seconds>	Sets the interval (in seconds) the access point uses to terminate its LAN interface if no activity is detected for the specified interval.
	trunking	<mode>	Enables or disables 802.11q Trunking over the access point LAN port.
	native-vlan-tag	<mode>	Defines the untagged/tagged 802.1q native VLAN mode for LAN1 and LAN2.
	auto-negotiation	<mode>	Enables or disables auto-negotiation for the access point LAN port.
	speed	<mbps>	Defines the access point LAN port speed as either 10 Mbps or 100 Mbps.
	duplex	<mode>	Defines the Access Port LAN port duplex as either half or full.
	username	<name>	Specifies user name for 802.1x port authentication over the LAN interface.
	passwd	<password>	The 0-32 character password for the username for the 802.1x port.
	ip-mode	<ip>	Defines the access point LAN port IP mode.
	ipadr	<ip>	Sets the IP address used by the LAN port.
	mask	<ip>	Defines the IP address used for access point LAN port network mask.
	dgw	<ip>	Sets the Gateway IP address used by the LAN port.
	domain	<name>	Specifies the domain name used by the access point LAN port.
	dns	<ip>	Sets the IP address of the primary and secondary DNS servers.
	wins	<ip>	Defines the IP address of the WINS server used by the LAN port.

Example

```
admin(network.lan)>
admin(network.lan)>set lan 1 enable
admin(network.lan)>set name 1 engineering
admin(network.lan)>set ethernet-port-lan 1
admin(network.lan)>set timeout 45
admin(network.lan)>set trunking 1 disable
admin(network.lan)>set native-vlan-tag 1 untagged
admin(network.lan)>set auto-negotiation disable
admin(network.lan)>set speed 100M
admin(network.lan)>set duplex full
admin(network.lan)>set dns 1 192.168.0.1
admin(network.lan)>set wins 1 192.168.0.254
admin(network.lan)>set trunking disable
admin(network.lan)>set username phil
admin(network.lan)>set passwd ea0258c1
```

For information on configuring the LAN using the applet (GUI), see “Configuring the LAN Interface” on page 123.

Network LAN, Bridge Commands

AP4700>admin(network.lan.bridge)>

Displays the access point Bridge submenu.

show	Displays the mesh configuration parameters for the access point’s LANs.
set	Sets the mesh configuration parameters for the access point’s LANs.
..	Moves to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI and exits the session.

For an overview of the access point’s mesh networking options using the applet (GUI), see “Configuring Mesh Networking Support” on page 581.

AP4700>admin(network.lan.bridge)>show

Displays the mesh bridge configuration parameters for the access point's LANs.

Syntax

show	Displays mesh bridge configuration parameters for the access point's LANs.

Example

```
admin(network.lan.bridge)>show

** LAN1 Bridge Configuration **
Bridge Priority              :63335
Hello Time (seconds)         :2
Message Age Time (seconds)   :20
Forward Delay Time (seconds) :15

Entry Ageout Time (seconds)  :300

** LAN2 Bridge Configuration **
Bridge Priority              :63335
Hello Time (seconds)         :2
Message Age Time (seconds)   :20
Forward Delay Time (seconds) :15

Entry Ageout Time (seconds)  :300
```

For an overview of the access point's mesh networking options using the applet (GUI), see "Configuring Mesh Networking Support" on page 581.

AP4700>admin(network.lan.bridge)>set

Sets the mesh configuration parameters for the access point’s LANs.

Syntax

set	priority	<LAN-idx>	<seconds>	Sets bridge priority time in seconds (0-65535) for specified LAN.
	hello	<LAN-idx>	<seconds>	Sets bridge hello time in seconds (0-10) for specified LAN.
	msgage	<LAN-idx>	<seconds>	Sets bridge message age time in seconds (6-40) for specified LAN.
	fwddelay	<LAN-idx>	<seconds>	Sets bridge forward delay time in seconds (4-30) for specified LAN.
	ageout	<LAN-idx>	<seconds>	Sets bridge forward table entry time in seconds (4-3600) for specified LAN.

Example

```
admin(network.lan.bridge)>set priority 2 63335
admin(network.lan.bridge)>set hello 2 2
admin(network.lan.bridge)>set msgage 2 20
admin(network.lan.bridge)>set fwddelay 2 15
admin(network.lan.bridge)>set ageout 2 300

admin(network.lan.bridge)>show

** LAN1 Mesh Configuration **
Bridge Priority              :63335
Hello Time (seconds)         :2
Message Age Time (seconds)   :20
Forward Delay Time (seconds) :15

Entry Ageout Time (seconds)  :300

** LAN2 Mesh Configuration **
Bridge Priority              :63335
Hello Time (seconds)         :2
Message Age Time (seconds)   :20
Forward Delay Time (seconds) :15

Entry Ageout Time (seconds)  :300
```

For an overview of the access point’s mesh networking options using the applet (GUI), see “Configuring Mesh Networking Support” on page 581.

Network LAN, WLAN-Mapping Commands

AP4700>admin(network.lan.wlan-mapping)>

Displays the WLAN/Lan/Vlan Mapping submenu.

show	Displays the VLAN list currently defined for the access point.
set	Sets the access point VLAN configuration.
create	Creates a new access point VLAN.
edit	Edits the properties of an existing access point VLAN.
delete	Deletes a VLAN.
lan-map	Maps access point existing WLANs to an enabled LAN.
vlan-map	Maps access point existing WLANs to VLANs.
..	Moves to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI and exits the session.

For an overview of the access point's VLAN configuration options using the applet (GUI), see "Configuring VLAN Support" on page 126.

AP4700>admin(network.lan.wlan-mapping)>show

Displays the VLAN list currently defined for the access point. These parameters are defined with the set command.

Syntax

show	name	Displays the existing list of VLAN names.
	vlan-cfg	Shows WLAN-VLAN mapping and VLAN configuration.
	lan-wlan	Displays a WLAN-LAN mapping summary.
	wlan	Displays the WLAN summary list.

Example

```
admin(network.lan.wlan-mapping)>show name
-----------------------------------------------------------------------------
Index     VLAN ID   VLAN Name
-----------------------------------------------------------------------------


1         1         VLAN_1
2         2         VLAN_2
3         3         VLAN_3
4         4         VLAN_4

admin(network.lan.wlan-mapping)>show vlan-cfg
-----------------------------------------------------------------------------
LAN No.     Management VLAN Tag      Native VLAN Tag
-----------------------------------------------------------------------------
      1                        1                   1
      2                        1                   1
          WLAN      :WLAN1
mapped to VLAN      :<none>
     VLAN Mode      :static

admin(network.lan.wlan-mapping)>show lan-wlan

WLANs on LAN1:
              :WLAN1
              :WLAN2
              :WLAN3
WLANs on LAN2:

admin(network.lan.wlan-mapping)>show wlan

WLAN1:
WLAN Name              :WLAN1
ESSID                  :101
Radio Bands            :2.4 and 5.0 GHz
VLAN                   :
Security Policy        :Default
QoS Policy             :Default
Rate Limiting          :disabled
```

For information on displaying the VLAN screens using the applet (GUI), see "Configuring VLAN Support" on page 126.

AP4700>admin(network.lan.wlan-mapping)>set

Sets VLAN parameters for the access point.

Syntax

set	mgmt- tag	<id>	Defines the Management VLAN tag index (1 or 2) to tag number (1-4095).
	native-tag	<id>	Sets the Native VLAN tag index (1 or 2) to tag number (1-4095).
	mode	<wlan-idx>	Sets WLAN VLAN mode (WLAN 1-16) to either dynamic or static.

Example

```
admin(network.lan.wlan-mapping)>set mgmt-tag 1 10
admin(network.lan.wlan-mapping)>set native-tag 1 12
admin(network.lan.wlan-mapping)>set mode 1 static

admin(network.lan.wlan-mapping)>show vlan-cfg

-----------------------------------------------------------------------------
LAN No.     Management VLAN Tag      Native VLAN Tag
-----------------------------------------------------------------------------
      1                         10                  12
      2                         1                   1
          WLAN      :WLAN1
mapped to VLAN      :<none>
     VLAN Mode      :static
```

For information on configuring VLANs using the applet (GUI), see "Configuring VLAN Support" on page 126.

AP4700>admin(network.lan.wlan-mapping)>create

Creates a VLAN for the access point.

Syntax

create	vlan-id	<id>	Defines the VLAN ID (1-4095).
	vlan-name	<name>	Specifies the name of the VLAN (1-31 characters in length).

Example

```
admin(network.lan.wlan-mapping)>
admin(network.lan.wlan-mapping)>create 5 vlan-5
```

For information on creating VLANs using the applet (GUI), see "Configuring VLAN Support" on page 126.

AP4700>admin(network.lan.wlan-mapping)>edit

Modifies a VLAN's name and ID.

Syntax

edit	name	<name>	Modifies an existing VLAN name (1-31 characters in length)
	id	<id>	Modifies an existing VLAN ID (1-4095) characters in length)

For information on editing VLANs using the applet (GUI), see "Configuring VLAN Support" on page 126.

AP4700>admin(network.lan.wlan-mapping)>delete

Deletes a specific VLAN or all VLANs.

Syntax

delete	< VLAN id>	Deletes a specific VLAN ID (1-16).
	all	Deletes all defined VLAN entries.

For information on deleting VLANs using the applet (GUI), see "Configuring VLAN Support" on page 126.

AP4700>admin(network.lan.wlan-mapping)>lan-map

Maps an access point VLAN to a WLAN.

Syntax

lan-map	<wlan name>	Maps an existing WLAN to an enabled LAN. All names and IDs are case-sensitive.
	<lan name>	Defines enabled LAN name. All names and IDs are case-sensitive.

Example

```
admin(network.lan.wlan-mapping)>lan-map wlan1 lan1
```

For information on mapping VLANs using the applet (GUI), see "Configuring VLAN Support" on page 126.

AP4700>admin(network.lan.wlan-mapping)>vlan-map

Maps an access point VLAN to a WLAN.

Syntax

vlan-map	<wlan name>	Maps an existing WLAN to an enabled LAN. All names and IDs are case-sensitive.
	<vlan name>	Defines the existing VLAN name. All names and IDs are case-sensitive.

Example

```
admin(network.lan.wlan-mapping)>vlan-map wlan1 vlan1
```

For information on mapping VLANs using the applet (GUI), see “Configuring VLAN Support” on page 126.

Network LAN, DHCP Commands

AP4700>admin(network.lan.dhcp)>

Displays the access point DHCP submenu. The items available are displayed below.

show	Displays DHCP parameters.
set	Sets DHCP parameters.
add	Adds static DHCP address assignments.
delete	Deletes static DHCP address assignments.
list	Lists static DHCP address assignments.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI and exits the session.

AP4700>admin(network.lan.dhcp)>show

Shows DHCP parameter settings.

Syntax

show	Displays DHCP parameter settings for the access point. These parameters are defined with the set command.

Example

```
admin(network.lan.dhcp)>show
**LAN1 DHCP Information**
DHCP Address Assignment Range:
     Starting IP Address  : 192.168.0.100
     Ending IP Address    : 192.168.0.254

Lease Time           : 86400

**LAN2 DHCP Information**
DHCP Address Assignment Range:
     Starting IP Address  : 192.168.0.100
     Ending IP Address    : 192.168.0.254

Lease Time           : 86400
```

For information on configuring DHCP using the applet (GUI), see “Configuring the LAN Interface” on page 123.

AP4700>admin(network.lan.dhcp)>set

Sets DHCP parameters for the LAN port.

Syntax

set	range	<LAN-idx>	<ip1>	<ip2>	Sets the DHCP assignment range from IP address <ip1> to IP address <ip2> for the specified LAN (1-lan1, 2-lan2).
	lease	<LAN-idx>	<lease>		Sets the DHCP lease time <lease> in seconds (1-999999) for the specified LAN.

Example

```
admin(network.lan.dhcp)>set range 1 192.168.0.100 192.168.0.254
admin(network.lan.dhcp)>set lease 1 86400

admin(network.lan.dhcp)>show
**LAN1 DHCP Information**
DHCP Address Assignment Range:
     Starting IP Address  : 192.168.0.100
     Ending IP Address    : 192.168.0.254

Lease Time           : 86400
```

For information on configuring DHCP using the applet (GUI), see “Configuring the LAN Interface” on page 123.

AP4700>admin(network.lan.dhcp)>add

Adds static DHCP address assignments.

Syntax

add	<LAN-idx>	<mac>	<ip>	Adds a reserved static IP address to a MAC address for the specified LAN.

Example

```
admin(network.lan.dhcp)>add 1 00A0F8112233 192.160.24.6
admin(network.lan.dhcp)>add 1 00A0F1112234 192.169.24.7
admin(network.lan.dhcp)>list 1

-----------------------------------------------------------------------------
Index   MAC Address     IP Address
-----------------------------------------------------------------------------

1      00A0F8112233   192.160.24.6
2      00A0F8112234   192.169.24.7
```

For information on adding client MAC and IP address information using the applet (GUI), see "Configuring Advanced DHCP Server Settings" on page 132.

AP4700>admin(network.lan.dhcp)>delete

Deletes static DHCP address assignments.

Syntax

delete	<LAN-idx>	<entry>	Deletes the static DHCP address entry (1-30) for the specified LAN.
	<LAN-idx>	all	Deletes all static DHCP addresses.

Example

```
admin(network.lan.dhcp)>list 1

-----------------------------------------------------------------------------
Index   MAC Address     IP Address
-----------------------------------------------------------------------------

1      00A0F8112233   10.1.2.4
2      00A0F8102030   10.10.1.2
3      00A0F8112234   10.1.2.3
4      00A0F8112235   192.160.24.6
5      00A0F8112236   192.169.24.7

admin(network.lan.dhcp)>delete 1

-----------------------------------------------------------------------------
index   mac address     ip address
-----------------------------------------------------------------------------

1      00A0F8102030   10.10.1.2
2      00A0F8112234   10.1.2.3
3      00A0F8112235   192.160.24.6
4      00A0F8112236   192.169.24.7

admin(network.lan.dhcp)>delete 1 all

-----------------------------------------------------------------------------
index   mac address     ip address
-----------------------------------------------------------------------------
```

For information on deleting client MAC and IP address information using the applet (GUI), see "Configuring Advanced DHCP Server Settings" on page 132.

AP4700>admin(network.lan.dhcp)>list

Lists static DHCP address assignments.

Syntax

list	<LAN-idx>	Lists the static DHCP address assignments for the specified LAN (1-LAN1, 2 LAN2).

Example

```
admin(network.lan.dhcp)>list 1

-----------------------------------------------------------------------------
Index   MAC Address     IP Address
-----------------------------------------------------------------------------


1      00A0F8112233   10.1.2.4
2      00A0F8102030   10.10.1.2
3      00A0F8112234   10.1.2.3
4      00A0F8112235   192.160.24.6
5      00A0F8112236   192.169.24.7

admin(network.lan.dhcp)>
```

For information on listing client MAC and IP address information using the applet (GUI), see "Configuring Advanced DHCP Server Settings" on page 132.

Network Type Filter Commands

AP4700>admin(network.lan.type-filter)>

Displays the access point Type Filter submenu. The items available under this command include:

show	Displays the current Ethernet Type exception list.
set	Defines Ethernet Type Filter parameters.
add	Adds an Ethernet Type Filter entry.
delete	Removes an Ethernet Type Filter entry.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.lan.type-filter)>show

Displays the access point’s current Ethernet Type Filter configuration.

Syntax

show	<LAN-idx>	Displays the existing Type-Filter configuration for the specified LAN.

Example

```
admin(network.lan.type-filter)>show 1

Ethernet Type Filter mode              : allow
-----------------------------------------------------------------------------
index                  ethernet type
-----------------------------------------------------------------------------
1                      8137
```

For information on displaying the type filter configuration using the applet, see “Setting the Type Filter Configuration” on page 133.

AP4700>admin(network.lan.type-filter)>set

Defines the access point Ethernet Type Filter configuration.

Syntax

set	mode	<LAN-idx>	<mode> allow or deny	Allows or denies the access point from processing a specified Ethernet data type for the specified LAN.

Example

```
admin(network.lan.type-filter)>set mode 1 allow
```

For information on configuring the type filter settings using the applet (GUI), see "Setting the Type Filter Configuration" on page 133.

AP4700>admin(network.lan.type-filter)>add

Adds an Ethernet Type Filter entry.

Syntax

add <LAN-idx>	<type>	Adds entered Ethernet Type to list of data types either allowed or denied access point processing permissions for the specified LAN (either LAN1 or LAN2).

Example

```
admin(network.lan.type-filter)>

admin(network.wireless.type-filter)>add 1 8137
admin(network.wireless.type-filter)>add 2 0806
admin(network.wireless.type-filter)>show 1

Ethernet Type Filter mode              : allow
-----------------------------------------------------------------------------
index                  ethernet type
-----------------------------------------------------------------------------
1                      8137
2                      0806
3                      0800
4                      8782
```

For information on configuring the type filter settings using the applet (GUI), see "Setting the Type Filter Configuration" on page 133.

AP4700>admin(network.lan.type-filter)>delete

Removes an Ethernet Type Filter entry individually or the entire Type Filter list.

Syntax

delete	<LAN-idx>	<index>	Deletes the specified Ethernet Type index entry (1 through 16).
	<LAN-idx>	all	Deletes all Ethernet entries currently in list.

Example

```
admin(network.lan.type-filter)>delete 1 1
admin(network.lan.type-filter)>show 1

Ethernet Type Filter mode              : allow
------------------------------------------------------------------------------
index                  ethernet type
------------------------------------------------------------------------------
1                      0806
2                      0800
3                      8782

admin(network.lan.type-filter)>delete 2 all
admin(network.lan.type-filter)>show 2

Ethernet Type Filter mode              : allow
------------------------------------------------------------------------------
index                  ethernet type
------------------------------------------------------------------------------
```

For information on configuring the type filter settings using the applet (GUI), see “Setting the Type Filter Configuration” on page 133.

Network WAN Commands

AP4700>admin(network.wan)>

Displays the WAN submenu. The items available under this command are shown below.

```
  show                              : show WAN, PPPoE and 3G WWAN configuration
  set                               : set WAN, PPPoE and 3G WWAN configuration
  delete                            : delete WWAN CRM Remote Gateways
  clear                             : clear WWAN AP name
                                    :
  nat                               : go to NAT menu
  vpn                               : go to VPN menu
  content                           : go to Outbound Content Filtering menu
  dyndns                            : go to dyndns menu
                                    :
  ..                                : go to parent menu
  /                                 : go to root menu
                                    :
  save                              : save cfg to system flash
  quit                              : quit cli
```

For an overview of the WAN configuration options using the applet (GUI), see "Configuring WAN Settings" on page 135.

AP4700>admin(network.wan)>show

Displays the access point WAN port parameters.

Syntax

show	Shows the general IP parameters for the WAN port along with settings for the WAN interface.

Example

```
admin(network.wan)>show

Status                            : enable
WAN DHCP Client Mode              : disable
IP Address                        : 10.1.1.1
Network Mask                      : 255.0.0.0
Default Gateway                   : 0.0.0.0
Primary DNS Server                : 0.0.0.0
Secondary DNS Server              : 0.0.0.0

Auto-negotiation                  : disable
Speed                             : 100M
Duplex                            : full

WAN IP 2                          : disable
WAN IP 3                          : disable
WAN IP 4                          : disable
WAN IP 5                          : disable
WAN IP 6                          : disable
WAN IP 7                          : disable
WAN IP 8                          : disable

PPPoE Mode                        : enable
PPPoE User Name                   : JohnDoe
PPPoE Password                    : *******
PPPoE keepalive mode              : enable
PPPoE Idle Time                   : 600
PPPoE Authentication Type         : chap
PPPoE State

admin(network.wan)>
```

For an overview of the WAN configuration options available using the applet (GUI), see "Configuring WAN Settings" on page 135.

AP4700>admin(network.wan)>set

Defines the configuration of the access point WAN port.

Syntax

set	wan	enable/disable		Enables or disables the access point WAN port.
	dhcp	enable/disable		Enables or disables WAN DHCP Client mode.
	ipadr	<idx>	<a.b.c.d>	Sets up to 8 (using <indx> from 1 to 8) IP addresses <a.b.c.d> for the access point WAN interface.
	mask	<a.b.c.d>		Sets the subnet mask for the access point WAN interface.
	dgw	<a.b.c.d>		Sets the default gateway IP address to <a.b.c.d>.
	dns	<idx>	<a.b.c.d>	Sets the IP address of one or two DNS servers, where <indx> indicates either the primary (1) or secondary (2) server, and <a.b.c.d> is the IP address of the server.
	auto-negotiation	enable/disable		Enables or disables auto-negotiation for the access point WAN port.
	speed	<mbps>		Defines the WAN port speed as either 10 Mbps or 100 Mbps.
	duplex	<mode>		Defines the Access Port WAN port duplex as either half or full.
	pppoe	<mode>	enable/disable	Enables or disables PPPoE.
		user	<name>	Sets PPPoE user name.
		passwd	<password>	Defines the PPPoE password.
		ka	enable/disable	Enables or disables PPPoE keepalive.
		idle	<time>	Sets PPPoE idle time.
		type	<auth-type>	Sets PPPoE authentication type.
	wwan	<mode>	enable/fail-over	Sets the 3G wireless WAN operations mode (disable/fail-over) for a defined user name, password and remote gateway.

Example

```
admin(network.wan)>
admin(network.wan)>set dhcp disable
admin(network.wan)>set ipadr 157.169.22.5
admin(network.wan)>set dgw 157.169.22.1
admin(network.wan)>set dns 1 157.169.22.2
admin(network.wan)>set auto-negotiation disable
admin(network.wan)>set speed 10M
admin(network.wan)>set duplex half
admin(network.wan)>set mask 255.255.255.000
admin(network.wan)>set pppoe mode enable
admin(network.wan)>set pppoe type chap
admin(network.wan)>set pppoe user jk
admin(network.wan)>set pppoe passwd @#$goodpassword%$#
admin(network.wan)>set pppoe ka enable
admin(network.wan)>set pppoe idle 600
admin(network.wan)>set wwan mode disable
```

For an overview of the WAN configuration options available using the applet (GUI), see “Configuring WAN Settings” on page 135.

Network WAN NAT Commands

AP4700>admin(network.wan.nat)>

Displays the NAT submenu. The items available under this command are shown below.

show	Displays the access point's current NAT parameters for the specified index.
set	Defines the access point NAT settings.
add	Adds NAT entries.
delete	Deletes NAT entries.
list	Lists NAT entries.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

For an overview of the NAT configuration options available using the applet (GUI), see "Configuring Network Address Translation (NAT) Settings" on page 141.

AP4700>admin(network.wan.nat)>show

Displays access point NAT parameters.

Syntax

show	<idx> <cr>	Displays access point NAT parameters for the specified NAT index (1-8).

Example

```
admin(network.wan.nat)>show 2

WAN IP Mode                         : enable
WAN IP Address                      : 157.235.91.2
NAT Type                            : 1-to-many
Inbound Mappings                    : Port Forwarding

unspecified port forwarding mode    : enable
unspecified port fwd. ip address    : 111.223.222.1
one to many nat mapping

-------------------------------------------------------------------------------
LAN No.               WAN IP
-------------------------------------------------------------------------------
1                    157.235.91.2
2                    157.235.91.2

admin(network.wan.nat)>
```

For an overview of the NAT options available using the applet (GUI), see "Configuring Network Address Translation (NAT) Settings" on page 141.

AP4700>admin(network.wan.nat)>set

Sets NAT inbound and outbound parameters.

Syntax

set	type	<index>	<type>	Sets the type of NAT translation for WAN address index <idx> (1-8) to <type> (none, 1-to-1, or 1-to-many).
	ip	<index>	<ip>	Sets NAT IP mapping associated with WAN address <idx> to the specified IP address <ip>.
	inb	<index>	<ip> <mode>	Sets inbound IP address for specified index <index> <ip address> Sets inbound mode for specified index <index> <enable/disable>
	outb	<index>	<ip> <from> <to>	Sets outbound IP address for specified index <index> <ip address> Sets outbound NAT destination <LAN1 or LAN2> <WAN ip 1-8 or None>.

Example

```
admin(network.wan.nat)>set type 2 1-to-many
admin(network.wan.nat)>set ip 2 10.1.1.1 (this command is used when NAT is 1-to-1)

admin(network.wan.nat)>show 2

WAN IP Mode                        : enable
WAN IP Address                     : 157.235.91.2
NAT Type                           : 1-to-many
Inbound Mappings                   : Port Forwarding

unspecified port forwarding mode   : enable
unspecified port fwd. ip address   : 111.223.222.1
one to many nat mapping

-------------------------------------------------------------------------------
LAN No.               WAN IP
-------------------------------------------------------------------------------
1                     157.235.91.2
2                     10.1.1.1
```

For an overview of the NAT options available using the applet (GUI), see "Configuring Network Address Translation (NAT) Settings" on page 141.

AP4700>admin(network.wan.nat)>add

Adds NAT entries.

Syntax

add <idx> <name> <tran> <port1> <port2> <ip> <dst_port>

Sets an inbound network address translation (NAT) for WAN address <idx>, where <name> is the name of the entry (1 to 7 characters), <tran> is the transport protocol (one of *tcp*, udp, icmp, ah, esp, gre, or all), <port1> is the starting port number in a port range, <port2> is the ending port number in a port range, <ip> is the internal IP address, and <dst_port> is the (optional) internal translation port.

Example

```
admin(network.wan.nat)>add 1 indoors udp 20 29 10.10.2.2

admin(network.wan.nat)>list 1
-----------------------------------------------------------------------------
index   name    Transport  start port   end port   internal ip     translation
-----------------------------------------------------------------------------
1       indoor  udp        20           29         10.10.2.2      0
```

For an overview of the NAT options available using the applet (GUI), see “Configuring Network Address Translation (NAT) Settings” on page 141.

AP4700>admin(network.wan.nat)>delete

Deletes NAT entries.

Syntax

delete	<idx>	<entry>	Deletes a specified NAT index entry <entry> associated with the WAN.
	<idx>	all	Deletes all NAT entries associated with the WAN.

Example

```
admin(network.wan.nat)>list 1
-----------------------------------------------------------------------------
index   name    Transport  start port   end port   internal ip     translation
-----------------------------------------------------------------------------
1       special tcp        20          21         192.168.42.16   21

admin(network.wan.nat)>delete 1 1
admin(network.wan.nat)>list 1
-----------------------------------------------------------------------------
index   name    Transport  start port   end port   internal ip     translation
-----------------------------------------------------------------------------
```

Related Commands:

add	Adds entries to the list of inbound NAT entries.
list	Displays the list of inbound NAT entries.

For an overview of the NAT options available using the applet (GUI), see "Configuring Network Address Translation (NAT) Settings" on page 141.

AP4700>admin(network.wan.nat)>list

Lists access point NAT entries for the specified index.

Syntax

list	<idx>	Lists the inbound NAT entries associated with the WAN index (1-8).

Example

```
admin(network.wan.nat)>list 1
-----------------------------------------------------------------------------
index    name     Transport  start port   end port    internal ip      translation
-----------------------------------------------------------------------------
1        special  tcp        20           21          192.168.42.16    21
```

Related Commands:

delete	Deletes inbound NAT entries from the list.
add	Adds entries to the list of inbound NAT entries.

For an overview of the NAT options available using the applet (GUI), see "Configuring Network Address Translation (NAT) Settings" on page 141.

AP4700>admin(network.wan.vpn)>

Displays the VPN submenu. The items available under this command include:

add	Adds VPN tunnel entries.
set	Sets key exchange parameters.
delete	Deletes VPN tunnel entries.
list	Lists VPN tunnel entries
reset	Resets all VPN tunnels.
stats	Lists security association status for the VPN tunnels.
ikestate	Displays an Internet Key Exchange (IKE) summary.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

For an overview of the VPN options available using the applet (GUI), see "Configuring VPN Tunnels" on page 225.

AP4700>admin(network.wan.vpn)>add

Adds a VPN tunnel entry.

Syntax

add <name>	<idx> <LWanIP> <RSubnetIP> <RSubnetMask> <RGatewayIP>
	Creates a tunnel <name> (1 to 13 characters) to gain access through local WAN IP <LWanIP> from the remote subnet with address <RSubnetIP> and subnet mask <RSubnetMask> using the remote gateway <RGatewayIP>.

Example

```
admin(network.wan.vpn)>add 2 SJSharkey 209.235.44.31 206.107.22.46 255.255.255.224
206.107.22.1
If tunnel type is Manual, proper SPI values and Keys must be configured after adding
the tunnel

admin(network.wan.vpn)>
```

For information on configuring VPN using the applet (GUI), see “Configuring VPN Tunnels” on page 225.

AP4700>admin(network.wan.vpn)>set

Sets VPN entry parameters.

Syntax

set	type	<name>	<tunnel type>		Sets the tunnel type <name> to Auto or Manual for the specified tunnel name.
	authalgo	<name>	<authalgo>		Sets the authentication algorithm for <name> to (None, MD5, or SHA1).
	authkey	<name>	<dir> <authkey>		Sets the AH authentication key (if type is Manual) for tunnel <name> with the direction set to IN or OUT, and the manual authentication key set to <authkey>. (The key size is 32 hex characters for MD5, and 40 hex characters for SHA1).
	esp-type	<name>	<esptype>		Sets the Encapsulating Security Payload (ESP) type. Options include None, ESP, or ESP-AUTH.
	esp-encalgo	<name>	<escalgo>		Sets the ESP encryption algorithm. Options include DES, 3DES, AES128, AES192, or AES256).
	esp-enckey	<name>	<dir> <enckey>		Sets the Manual Encryption Key in ASCII for tunnel <name> and direction **IN** or **OUT** to the key <enc-key>. The size of the key depends on the encryption algorithm. - 16 hex characters for DES - 48 hex characters for 3DES - 32 hex characters for AES128 - 48 hex characters for AES192 - 64 hex characters for AES256
	esp-authalgo	<name>	<authalgo>		Sets the ESP authentication algorithm. Options include MD5 or SHA1.
	esp-authkey	<name>	<dir> <authkey>		Sets ESP Authentication key <name> either for IN or OUT direction to <auth-key>, an ASCII string of hex characters. If authalgo is set to MD5, then provide 32 hex characters. If authalgo is set to SHA1, provide 40 hex characters.
	spi	<name>	<algo> <dir>	<value>	Sets 6 character IN(bound) or OUT(bound) for AUTH (Manual Authentication) or ESP for <name> to <spi> (a hex value more than 0xFF) <value>.
	usepfs	<name>	<mode>		Enables or disables Perfect Forward Secrecy for <name>.
	salife	<name>	<lifetime>		Defines the name of the tunnnel <name> the Security Association Life Time <300-65535> applies to in seconds.

ike	opmode	<name>	<opmode>	Sets the Operation Mode of IKE for <name> to Main or Aggr(essive).
	myidtype	<name>	<idtype>	Sets the Local ID type for IKE authentication for <name> (1 to 13 characters) to <idtype> (IP, FQDN, or UFQDN).
	remidtype	<name>	<idtype>	Sets the Remote ID type for IKE authentication for <name> (1 to 13 characters) to <idtype> (IP, FQDN, or UFQDN).
	myiddata	<name>	<idtype>	Sets the Local ID data for IKE authentication for <name> to <idtype>. This value is not required when the ID type is set to IP.
	remiddata	<name>	<idtype>	Sets the Local ID data for IKE authentication for <name> to <idtype>. This value is not required when the ID type is set to IP.
	authtype	<name>	<authtype >	Sets the IKE Authentication type for <name> to <authtype> (PSK or RSA).
	authalgo	<name>	<authalgo >	Sets the IKE Authentication Algorithm for <name> to MD5 or SHA1.
	phrase	<name>	<phrase>	Sets the IKE Authentication passphrase for <name> to <phrase>.
	encalgo	<name>	<encalgo>	Sets the IKE Encryption Algorithm for <name> to <encalgo> (one of DES, 3DES, AES128, AES192, or AES256).
	lifetime	<name>	<lifetime>	Sets the IKE Key life time in seconds for <name> to <lifetime>.
	group	<name>	<group>	Sets the IKE Diffie-Hellman Group for <name> to either G768 or G1024.

For information on configuring VPN using the applet (GUI), see "Configuring VPN Tunnels" on page 225.

AP4700>admin(network.wan.vpn)>delete

Deletes VPN tunnel entries.

Syntax

delete	all	Deletes all VPN entries.
	<name>	Deletes VPN entries <name>.

Example

```
admin(network.wan.vpn)>list
--------------------------------------------------------------------------
Tunnel Name   Type    Remote IP/Mask     Remote Gateway  Local WAN IP
--------------------------------------------------------------------------
Eng2EngAnnex  Manual  192.168.32.2/24    192.168.33.1    192.168.24.198
SJSharkey     Manual  206.107.22.45/27   206.107.22.2    209.235.12.55

admin(network.wan.vpn)>delete Eng2EngAnnex
admin(network.wan.vpn)>list
--------------------------------------------------------------------------
Tunnel Name   Type    Remote IP/Mask     Remote Gateway  Local WAN IP
--------------------------------------------------------------------------
SJSharkey     Manual  206.107.22.45/27   206.107.22.2    209.235.12.55

admin(network.wan.vpn)>
```

For information on configuring VPN using the applet (GUI), see “Configuring VPN Tunnels” on page 225.

AP4700>admin(network.wan.vpn)>list

Lists VPN tunnel entries.

Syntax

list	<cr>	Lists all tunnel entries.
	<name>	Lists detailed information about tunnel named <name>. The <name> must match case with the name of the VPN tunnel entry.

Example

```
admin(network.wan.vpn)>list
--------------------------------------------------------------------------
Tunnel Name   Type    Remote IP/Mask     Remote Gateway  Local WAN IP
--------------------------------------------------------------------------
Eng2EngAnnex  Manual  192.168.32.2/24    192.168.33.1    192.168.24.198
SJSharkey     Manual  206.107.22.45/27   206.107.22.2    209.235.12.55

admin(network.wan.vpn)>list SJSharkey
--------------------------------------------------------------------------
Detail listing of VPN entry:
--------------------------------------------------------------------------
Name                     : SJSharkey
Local Subnet             : 1
Tunnel Type              : Manual
Remote IP                : 206.107.22.45
Remote IP Mask           : 255.255.255.224
Remote Security Gateway  : 206.107.22.2
Local Security Gateway   : 209.239.160.55
AH Algorithm             : None
Encryption Type          : ESP
Encryption Algorithm     : DES
ESP Inbound SPI          : 0x00000100
ESP Outbound SPI         : 0x00000100
```

For information on displaying VPN information using the applet (GUI), see “Viewing VPN Status” on page 238.

AP4700>admin(network.wan.vpn)>reset

Resets all of the access point’s VPN tunnels.

Syntax

reset	Resets all VPN tunnel states.

Example

```
admin(network.wan.vpn)>reset
VPN tunnels reset.
admin(network.wan.vpn)>
```

For information on configuring VPN using the applet (GUI), see “Configuring VPN Tunnels” on page 225.

AP4700>admin(network.wan.vpn)>stats

Lists statistics for all active tunnels.

Syntax

stats	Display statistics for all VPN tunnels.

Example

```
admin(network.wan.vpn)>stats
-----------------------------------------------------------------------------
Tunnel Name   Status     SPI(OUT/IN)       Life Time        Bytes(Tx/Rx)
-----------------------------------------------------------------------------
Eng2EngAnnex  Not Active
SJSharkey     Not Active
```

For information on displaying VPN information using the applet (GUI), see “Viewing VPN Status” on page 238.

AP4700>admin(network.wan.vpn)>ikestate

Displays statistics for all active tunnels using Internet Key Exchange (IKE).

Syntax

ikestate	Displays status about Internet Key Exchange (IKE) for all tunnels. In particular, the table indicates whether IKE is connected for any of the tunnels, it provides the destination IP address, and the remaining lifetime of the IKE key.

Example

```
admin(network.wan.vpn)>ikestate
----------------------------------------------------------------------
Tunnel Name   IKE State            Dest IP         Remaining Life
----------------------------------------------------------------------
Eng2EngAnnex  Not Connected        ----            ---
SJSharkey     Not Connected        ----            ---

admin(network.wan.vpn)>
```

For information on configuring IKE using the applet (GUI), see “Configuring IKE Key Settings” on page 235.

AP4700>admin(network.wan.content)>

Displays the Outbound Content Filtering menu. The items available under this command include:

addcmd	Adds control commands to block outbound traffic.
delcmd	Deletes control commands to block outbound traffic.
list	Lists application control commands.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wan.content)>addcmd

Adds control commands to block outbound traffic.

Syntax

addcmd	web		Adds WEB commands to block outbound traffic.
		proxy	Adds a Web proxy command.
		activex	Adds activex files.
		file	Adds Web URL extensions (10 files maximum)
	smtp		Adds SMTP commands to block outbound traffic.
		helo	helo command
		mail	mail command
		rcpt	rcpt command
		data	data command
		quit	quit command
		send	send command
		saml	saml command
		reset	reset command
		vrfy	vrfy command
		expn	expn command
	ftp		Adds FTP commands to block outbound traffic.
		put	store command
		get	retreive command
		ls	directory list command
		mkdir	create directory command
		cd	change directory command
		pasv	passive mode command

Example

```
admin(network.wan.content)>addcmd web proxy
admin(network.wan.content)>addcmd smtp data
admin(network.wan.content)>addcmd ftp put
```

AP4700>admin(network.wan.content)>delcmd

Deletes control commands to block outbound traffic.

Syntax

delcmd	web		Deletes WEB commands to block outbound traffic.
		proxy	Deletes a Web proxy command.
		activex	Deletes activex files.
		file	Deletes Web URL extensions (10 files maximum)
	smtp		Deletes SMTP commands to block outbound traffic.
		helo	helo command
		mail	mail command
		rcpt	rcpt command
		data	data command
		quit	quit command
		send	send command
		saml	saml command
		reset	reset command
		vrfy	vrfy command
		expn	expn command
	ftp		Deletes FTP commands to block outbound traffic.
		put	store command
		get	retreive command
		ls	directory list command
		mkdir	create directory command
		cd	change directory command
		pasv	passive mode command

Example

```
admin(network.wan.content)>delcmd web proxy
admin(network.wan.content)>delcmd smtp data
admin(network.wan.content)>delcmd ftp put
```

AP4700>admin(network.wan.content)>list

Lists application control commands.

Syntax

list	web	Lists WEB application control record.
	smtp	Lists SMTP application control record.
	ftp	Lists FTP application control record.

Example

```
admin(network.wan.content)>list web

HTTP Files/Commands
Web Proxy                   : deny
ActiveX                     : allow
filename                    :

admin(network.wan.content)>list smtp

SMTP Commands
HELO                   : deny
MAIL                   : allow
RCPT                   : allow
DATA                   : deny
QUIT                   : allow
SEND                   : allow
SAML                   : allow
RESET                  : allow
VRFY                   : allow
EXPN                   : allow

admin(network.wan.content)>list ftp

FTP Commands
Storing Files          : deny
Retreiving Files       : allow
Directory Files        : allow
Create Directory       : allow
Change Directory       : allow
Passive Operation      : allow
```

Network WAN, Dynamic DNS Commands

AP4700>admin(network.wan.dyndns)>

Displays the Dynamic DNS submenu. The items available under this command include:

```
  set                                : set dyndns parameters
  update                             : manual dyndns update
  show                               : show dyndns parameters
  save                               : save cfg to system flash
  quit                               : quit cli
  ..                                 : go to parent menu
  /                                  : go to root menu
```

For an overview of the Dynamic DNS options available using the applet (GUI), see “Configuring Dynamic DNS” on page 145.

AP4700>admin(network.wan.dyndns)>set

Sets the access point's Dynamic DNS configuration.

Syntax

set	mode	enable/disable	Enables or disbales the Dynamic DNS service for the access point.
	username	<name>	Enter a 1–32 character username for the account used for the access point.
	password	<password>	Enter a 1–32 character password for the account used for the access point.
	hostname	<host>	Enter a 1–32 character hostname for the account used for the access point.

Example

```
admin(network.wan.dyndns)>set mode enable
admin(network.wan.dyndns)>set username percival
admin(network.wan.dyndns)>set password mudskipper
admin(network.wan.dyndns)>set host greengiant
```

For an overview of the Dynamic DNS options available using the applet (GUI), see "Configuring Dynamic DNS" on page 145.

AP4700>admin(network.wan.dyndns)>update

Updates the access point's current WAN IP address with the DynDNS service.

Syntax

update	Updates the access point's current WAN IP address with the DynDNS service.

Example

```
admin(network.wan.dyndns)>update

IP Address                    : 157.235.91.231
Hostname                      : greengiant
```

For an overview of the Dynamic DNS options available using the applet (GUI), see "Configuring Dynamic DNS" on page 145.

AP4700>admin(network.wan.dyndns)>show

Shows the current Dynamic DNS configuration.

Syntax

show	Shows the access point's current Dynamic DNS configuration.

Example

```
admin(network.wan.dyndns)>show

DynDNS Configuration

Mode                         : enable
Username                     : percival
Password                     : ********
Hostname                     : greengiant

DynDNS Update Response

IP Address                   : 157.235.91.231
Hostname                     : greengiant
Status                       : OK
```

For an overview of the Dynamic DNS options available using the applet (GUI), see "Configuring Dynamic DNS" on page 145.

Network Wireless Commands

AP4700>admin(network.wireless)

Displays the access point wireless submenu. The items available under this command include:

set	Sets the access point’s wireless (proxy arp) configuration.
show	Displays the access point’s wireless (proxy arp) configuration.
wlan	Displays the WLAN submenu used to create and configure up to 16 WLANs per access point.
security	Displays the security submenu used to create encryption and authentication based security policies for use with access point WLANs.
acl	Displays to the *Access Control List* (ACL) submenu to restrict or allow MU access to access point WLANs.
radio	Displays the radio configuration submenu used to specify how the 802.11a/n or 802.11b/g radio is used with specific WLANs.
qos	Displays the *Quality of Service* (QoS) submenu to prioritize specific kinds of data traffic within a WLAN.
rate-limiting	Displays the Rate Limiting submenu.
rogue-ap	Displays the Rogue-AP submenu to configure devices located by the access point as friendly or threatening for interoperablity.
wips	Goes to the *Wireless Intrusion Protection System* (WIPS) submenu.
mu-locationing	Displays the MU locationing submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless)>set

Sets the access point’s wireless (proxy arp) configuration.

Syntax

show	<mode>	enable/disable	Enables/disables proxy-arp support.

Example

```
admin(network.wireless)>set proxy-arp enable
```

For informarton on configuring proxy arp support using the applet (GUI), see “Enabling Wireless LANs (WLANs)” on page 146.

AP4700>admin(network.wireless)>show

Displays the access point’s wireless (proxy arp) configuration.

Syntax

show	Displays the access point’s wireless (proxy arp) configuration.

Example

```
admin(network.wireless)>show

Proxy ARP                         : dynamic
```

For informarton on configuring proxy arp support using the applet (GUI), see “Enabling Wireless LANs (WLANs)” on page 146.

Network WLAN Commands

AP4700>admin(network.wireless.wlan)>

Displays the access point wireless LAN (WLAN) submenu. The items available under this command include:

show	Displays the access point's current WLAN configuration.
create	Defines the parameters of a new WLAN.
edit	Modifies the properties of an existing WLAN.
delete	Deletes an existing WLAN.
hotspot	Displays the WLAN hotspot menu.
ipfpolicy	Goes to the WLAN IP Filter Policy menu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

For an overview of the Wireless configuration options available to the using the applet (GUI), see "Enabling Wireless LANs (WLANs)" on page 146.

AP4700>admin(network.wireless.wlan)>show

Displays the access point’s current WLAN configuration.

Syntax

show	summary		Displays the current configuration for existing WLANs.
	wlan	<number>	Displays the configuration for the requested WLAN (WLAN 1 through 16).

Example

```
admin(network.wireless.wlan)>show summary

WLAN1
WLAN Name                          : Lobby
ESSID                              : 101
Radio Band(s)                      : 2.4 and 5.0 GHz
VLAN                               : <none>
Security Policy                    : Default
QoS Policy                         : Default
Rate Limiting                      : disabled

admin(network.wireless.wlan)>show wlan 1

ESS Identifier                     : 101
WLAN Name                          : Lobby
802.11n (5.0 GHz) Radio            : available
802.11n (2.4 GHz) Radio            : not available
Client Bridge Mesh Backhaul        : available
Hotspot                            : not available
Maximum MUs                        : 127
MU Idle Timeout                    : 30
Security Policy                    : Default
MU Access Control                  : Default
Kerberos User Name                 :
Kerberos Password                  : ********
disallow mu to mu                  : disable
Use Secure Beacon                  : disable
answer Broadcast ess               : enable
QoS Policy                         : Default
per-mu rate limiting               : disabled
per-mu rate limit (wired-to-wl)    : 1000 kb
per-mu rate limit (wl-to-wired)    : 1000 kb
```

For information on displaying WLAN infromation using the applet (GUI), see “Enabling Wireless LANs (WLANs)” on page 146.

AP4700>admin(network.wireless.wlan)>create

Defines the parameters of a new WLAN.

Syntax

create				
	show	wlan	<number>	Displays newly created WLAN and policy number.
	set	ess	<essid>	Defines the ESSID for a target WLAN.
		wlan-name	<name>	Determines the name of this particlular WLAN (1-32).
		5.0GHz	<mode>	Enables or disables access to the access point 5.0 GHz radio.
		2.4Ghz	<mode>	Enables or disables access to the access point 2.4 GHz radio.
		mesh	<mode>	Enables or disables the Client Bridge Mesh Backhaul option.
		hotspot	<mode>	Enables or disables the Hotspot mode.
		max-mu	<number>	Defines the maximum number of MU able to operate within the WLAN (default = 127 MUs).
		idle- timeout	<minutes>	Sets the interval the access point uses to timeout idle MUs from WLAN inclusion. Set between 1 -65532 minutes. Default is 30 minutes.
		security	<name>	Sets the security policy to the WLAN (1-32).
		acl	<name>	Sets the MU ACL policy to the WLAN (1-32).
		passwd	<ascii string>	Defines a Kerberos password used if the WLAN's security policy uses a Kerberos server-based authentication scheme.
		no-mu-mu	<mode>	Enables or disables MUs associated to the same WLAN to not communicate with each other.
		sbeacon	<mode>	Enables or disables the AP from transmitting the ESSID in the beacon.
		bcast	<mode>	Enables or disables the access point from accepting broadcast IDs from MUs. Broadcast IDs are transmitted without security.
		qos	<name>	The index name representing the QoS policy used with this WLAN.
	add-wlan			Apply the changes to the modified WLAN and exit.
		rate-limiting	<mode>	Enables or disables MU Rate Limiting
		limit w2wl	<rate limit>	Sets the per-mu rate limit in kb (in the wired-to-wireless direction)
		limit wl2w	<rate limit>	Sets the per-mu rate limit in kb (in the wireless-to-wired direction)

Example

```
admin(network.wireless.wlan.create)>show wlan

ESS Identifier                      :
WLAN Name                           :
802.11n (5.0 GHz) Radio             : available
802.11n (2.4 GHz) Radio             : not available
```

```
Client Bridge Mesh Backhaul       : not available
Hotspot                           : not available
Maximum MUs                       : 127
MU Idle Timeout                   : 30
Security Policy                   : Default
MU Access Control                 :
Kerberos User Name                : Default
Kerberos Password                 : ********
disallow MU to MU                 : disable
Use Secure Beacon                 : disable
answer Broadcast ess              : disable
QoS Policy                        : Default
per-mu rate limiting              : disabled
per-mu rate limit (wired-to-wl)   : 1000 kb
per-mu rate limit (wl-to-wired)   : 1000 kb

admin(network.wireless.wlan.create)>show security
----------------------------------------------------------------------
Secu Policy Name      Authen      Encryption      Associated WLANs
----------------------------------------------------------------------
1 Default             Manual      no encrypt      Front Lobby
2 WEP Demo            Manual      WEP 64          2nd Floor
3 Open                Manual      no encrypt      1st Floor

WPA Countermeasure    enable

admin(network.wireless.wlan.create)>show acl
----------------------------------------------------------------------
ACL Policy Name            Associated WLANs
----------------------------------------------------------------------
1 Default                  Front Lobby
2 Admin                    3rd Floor
3 Demo Room                5th Floor

admin(network.wireless.wlan.create)>show qos
----------------------------------------------------------------------
QOS Policy Name            Associated WLANs
----------------------------------------------------------------------
1 Default                  Front Lobby
2 Voice                    Audio Dept
3 Video                    Video Dept
```

The CLI treats the following as invalid characters, thus they should not be used in the creation of an ESSID (or other):

```
' " \ & $ ^ * + ? [ ( { | , < >
```

For information on creating a WLAN using the applet (GUI), see “Creating/Editing Individual WLANs” on page 148.

AP4700>admin(network.wireless.wlan)>edit

Edits the properties of an existing WLAN policy.

Syntax

edit	<index>	Edits the properties of an existing (and specified) WLAN policy (1 -16).
	show	Displays the WLANs pamaters and summary.
	set	Edits the same WLAN parameters that can be modified using the create command.
	change	Completes the WLAN edits and exits the CLI session.
	..	Cancel the WLAN edits and exit the CLI session.

For information on editing a WLAN using the applet (GUI), see "Creating/Editing Individual WLANs" on page 148.

AP4700>admin(network.wireless.wlan)>delete

Deletes an existing WLAN.

Syntax

delete	<wlan-name>	Deletes a target WLAN using the name supplied.
	all	Deletes all WLANs defined (except default WLAN).

For information on deleting a WLAN using the applet (GUI), see "Creating/Editing Individual WLANs" on page 148.

AP4700>admin(network.wireless.wlan.hotspot)>

Displays the Hotspot submenu. The items available under this command include:

show	Show hotspot parameters.
redirection	Goes to the hotspot redirection menu.
radius	Goes to the hotspot RADIUS menu.
white-list	Goes to the hotspot white-list menu.
set	Sets the WLAN's hotspot configuration.
hs_import	Imports hotspot configuraiton files from a dedicated server.
hs_export	Exports hotspot configuraiton files to a dedicated server.
default	Stores default hotspot configuration files for a specified WLAN.
delete	Deletes hotspot files supporting a specified WLAN.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring the Hotspot options available to the using the applet (GUI), see "Configuring WLAN Hotspot Support" on page 160.

AP4700>admin(network.wireless.wlan.hotspot)>show

Displays the current access point Rogue AP detection configuration.

Syntax

show	hotspot	<idx>	Shows hotspot parameters per wlan index (1-16).

Example

```
admin(network.wireless.wlan.hotspot)>show hotspot 1

WLAN1
Hotspot Mode                      : enable
Hotspot Page Location             : default
External Login URL                : www.sjsharkey.com
External Welcome URL              :
External Fail URL                 :

Primary Server Ip adr             :157.235.21.21
Primary Server Port               :1812
Primary Server Secret             :******
Secondary Server Ip adr           :157.235.32.12
Secondary Server Port             :1812
Secondary Server Secret           :******
Accounting Mode                   :disable
Accounting Server Ip adr          :0.0.0.0
Accounting Server Port            :1813
Accounting Server Secret          :********
Accoutning Timeout                :10
Accoutning Retry-count            :3
Session Timeout Mode              :enable
Session Timeout                   :15

Whitelist Rules
-----------------------------------------------------------------------------
            Idx            IP Address
-----------------------------------------------------------------------------
            1              157.235.121.12
HOTSPOT CONFIGURATION PARAMETERS
customized filename               : login.html
cfg filepath                      :
server ip address                 : 157.235.21.21
user name                         : mudskipper
password                          : **********
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see "Configuring WLAN Hotspot Support" on page 160.

AP4700>admin(network.wireless.wlan.hotspot)>redirection

Goes to the hotspot redirection menu.

Syntax

redirection	set	<page-loc>	Sets the hotspot http-re-direction by index (1-16) for the specified URL.
		<exturl>	Shows hotspot http-redirection details for specifiec index (1-16) for specified page (login, welcome, fail) and target URL.
	show		Shows hotspot http-redirection details.
	save		Saves the updated hotspot configuration to flash memory.
	quit		Quits the CLI session.
	..		Goes to the parent menu.
	/		Goes to the root menu.

Example

```
admin(network.wireless.wlan.hotspot.redirection)>set page-loc 1 www.sjsharkey.com
admin(network.wireless.wlan.hotspot.redirection)>set exturl 1 fail www.sjsharkey.com
```

For information on configuring the hotspot options available to the access point using the applet (GUI), see “Configuring WLAN Hotspot Support” on page 160.

AP4700>admin(network.wireless.wlan.hotspot)>radius

Goes to the hotspot RADIUS menu.

Syntax

set	Sets the RADIUS hotspot configuration.
show	Shows RADIUS hotspot server details.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring the Hotspot options available to the access point using the applet (GUI), see "Configuring WLAN Hotspot Support" on page 160.

AP4700>admin(network.wireless.wlan.hotspot.radius)>set

Sets the RADIUS hotspot configuration.

Syntax

set	server	<idx>	<srvr_type>	<ipadr>	Sets the RADIUS hotpost server IP address per wlan index (1-16)
	port	<idx>	<srvr_type>	<port>	Sets the RADIUS hotpost server port per wlan index (1-16)
	secret	<idx>	<srvr_type>	<secret>	Sets the RADIUS hotspot server shared secret password.
	acct-mode	<idx>	<mode>		Sets the RADIUS hotspot server accounting mode (enable/disable)
	acct-server	<idx>	<ipadr>		Sets the RADIUS hotspot accounting server IP address per wlan index (1-16).
	acct-port	<idx>	<port>		Sets the RADIUS hotspot accounting server port per wlan index (1-16).
	acct-secret	<idx>	<secret>		Sets the RADIUS hotspot server shared secret password per wlan index (1-16).
	acct-timeout	<idx>	<timeout>		Sets the RADIUS hotspot server accounting timeout period in seconds (1-25).
	acct-retry	<idx>	<retry_count>		Sets the RADIUS hotspot server accounting accounting retry interval (1-10).
	sess-mode	<idx>	<mode>		Enables or disbales the use of a hotspot timeout interval for the specified wlan index (1-16).
	sess-timeout	<idx>	<timeout>		Sets the RADIUS hotspot server timeout interval for the specified index (1-16) between 15-180 minutes.

Example

```
admin(network.wireless.wlan.hotspot.radius)>set server 1 primary 157.235.121.1
admin(network.wireless.wlan.hotspot.radius)>set port 1 primary 1812
admin(network.wireless.wlan.hotspot.radius)>set secret 1 primary sjsharkey
admin(network.wireless.wlan.hotspot.radius)>set acct-mode 1 enable
admin(network.wireless.wlan.hotspot.radius)>set acct-server 1 157.235.14.14
admin(network.wireless.wlan.hotspot.radius)>set acct-port 1 1812
admin(network.wireless.wlan.hotspot.radius)>set acct-secret 1 londonfog
admin(network.wireless.wlan.hotspot.radius)>set acct-timeout 1 25
admin(network.wireless.wlan.hotspot.radius)>set acct-retry 1 10
admin(network.wireless.wlan.hotspot.radius)>set sess-mode 1 enable
admin(network.wireless.wlan.hotspot.radius)>set sess-timeout 1 15
```

For information on configuring the Hotspot options available to the access ointusing the applet (GUI), see “Configuring WLAN Hotspot Support” on page 160.

AP4700>admin(network.wireless.wlan.hotspot.radius)>show

Shows RADIUS hotspot server details.

Syntax

show	radius	<idx>	Displays RADIUS hotspot server details per index (1-16)

Example

```
admin(network.wireless.wlan.hotspot.radius)>show radius 1
WLAN 1
Hotspot Mode                         : enable
Primary Server Ip adr                : 157.235.12.12
Primary Server Port                  : 1812
Primary Server Secret                : ******
Secondary Server Ip adr              : 0.0.0.0
Secondary Server Port                : 1812
Secondary Server Secret              : ******
Accounting Mode                      : enable
Accounting Server Ip adr             : 157.235.15.16
Accounting Server Port               : 1813
Accounting Server Secret             : ******
Accounting Timeout                   : 10
Accounting Retry-count               : 3
Session Timeout Mode                 : enable

admin(network.wireless.wlan.hotspot.radius)>
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see “Configuring WLAN Hotspot Support” on page 160.

AP4700>admin(network.wireless.wlan.hotspot)>white-list

Goes to the hotspot white-list menu.

Syntax

white-list	add	<rule>	Adds hotspot whitelist rules by index (1-16) for specified IP address.
	clear		Clears hotspot whitelist rules for specified index (1-16).
	show		Shows hotspot whitelist rules for specified index (1-16).
	save		Saves the updated hotspot configuration to flash memory.
	quit		Quits the CLI session.
	..		Goes to the parent menu.
	/		Goes to the root menu.

Example

```
admin(network.wireless.wlan.hotspot.whitelist)>add rule 1 157.235.21.21
admin(network.wireless.wlan.hotspot.whitelist)>show white-rule 1

WLAN 1
Hotspot Mode                          disable
WhiteList Rules
--------------------------------------------------------------------------------
Idx                                   IP Address
--------------------------------------------------------------------------------
1                                     157.235.21.21
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see “Configuring WLAN Hotspot Support” on page 160.

AP4700>admin(network.wireless.wlan.hotspot)>set

Goes to the hotspot white-list menu.

Syntax

set	file	<wlan-idx> <file1> <file2>	Sets the hotspot customized file name(s) for the specified WLAN index <wlan-idx>. There’s a maximum of 10 files and file names should be separated by a space.
	path	<path>	Sets the 0 to 39 character path name used to route imported and exported hotspot files.
	server	<ipadr>	Sets the IP address of the server used to import and export hotspot files with the access point.
	user	<name>	Defines the user accessing the server supporting the access point’s hotspot.
	passwd	<passwd>	Establishes a password for the user.
	..		Goes to the parent menu.
	/		Goes to the root menu.

Example

```
admin(network.wireless.wlan.hotspot)>set file 2 login.html
admin(network.wireless.wlan.hotspot)>set path \\ftp:shareddrive/
admin(network.wireless.wlan.hotspot)>set server 157.235.112.1
admin(network.wireless.wlan.hotspot)>set user george
admin(network.wireless.wlan.hotspot)>set passwd just4you
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see “Configuring WLAN Hotspot Support” on page 160.

AP4700>admin(network.wireless.wlan.hotspot)>hs_import

Imports hotspot configuration parameters for a specified WLAN index <wlan-idx>.

Syntax

hs_import	<wlan-idx>	Imports hotspot configuration parameters for a specified WLAN index <wlan-idx> (1-16).

Example

```
admin(network.wireless.wlan.hotspot)>hs_import 2

Import Operation                  : [Started]
File Transfer                     : [In Progress]

File Transfer                     : [Completed]
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see "Configuring WLAN Hotspot Support" on page 160.

AP4700>admin(network.wireless.wlan.hotspot)>hs_export

Exports hotspot configuration parameters for a specified WLAN index <wlan-idx>.

Syntax

hs_export	<wlan-idx>	Exports hotspot configuration parameters for a specified WLAN index <wlan-idx> (1-16).

Example

```
admin(network.wireless.wlan.hotspot)>hs_export 2

Export Operation                   : [Started]
File Transfer                      : [In Progress]

File Transfer                      : [Completed]
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see "Configuring WLAN Hotspot Support" on page 160

AP4700>admin(network.wireless.wlan.hotspot)>default

Restores default hotspot files to a specified WLAN index <wlan-idx>.

Syntax

default	<wlan-idx>	Restores default hotspot files to a specified WLAN index <wlan-idx>.

Example

```
admin(network.wireless.wlan.hotspot)>default 2
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see "Configuring WLAN Hotspot Support" on page 160.

AP4700>admin(network.wireless.wlan.hotspot)>delete

Deletes hotspot files from a specified WLAN index <wlan-idx>.

Syntax

delete	<wlan-idx>	Deletes hotspot files from a specified WLAN index <wlan-idx>.

Example

```
admin(network.wireless.wlan.hotspot)>delete 2
Warning: This will delete all the files from the corresponding directory.
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see "Configuring WLAN Hotspot Support" on page 160.

AP4700>admin(network.wireless.security)>

Displays the access point wireless security submenu. The items available under this command include:

show	Displays the access point's current security configuration.
set	Enables/disables the WPA countermeasure.
create	Creates a security policy.
edit	Edits the properties of an existing security policy.
delete	Removes a specific security policy.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

For information on the security configuration options available to the access point using the applet (GUI), see "Configuring Security Options" on page 197.

AP4700>admin(network.wireless.security)>show

Displays the access point's current security configuration.

Syntax

show	summary		Displays list of existing security policies (1-16).
	policy	<id>	Displays the specified security policy <id>.

Example

```
admin(network.wireless.security)>show summary

----------------------------------------------------------------------
Secu Policy Name      Authen      Encryption      Associated WLANs
----------------------------------------------------------------------
1 Default             Manual      no encrypt      Lobby
2 WEP Demo            Manual      WEP 64          2nd Floor
3 Open                Manual      no encrypt      1st Floor

WPA Countermeasure    enable

admin(network.wireless.security)>show policy 1

Policy Name                       : Default
Authentication type               : Manual Pre-shared key/No authentication

Encryption type                   : no encryption
```

Related Commands:

create	Defines security parameters for the specified WLAN.

For information displaying existing WLAN security settings using the applet (GUI), see "Enabling Authentication and Encryption Schemes" on page 200.

AP4700>admin(network.wireless.security)>set

Enables/disables the WPA countermeasure.

Syntax

set	<mode>	Enables/disables WPA countermeasures.

Example

```
admin(network.wireless.security)set wpa-countermeasure enable
admin(network.wireless.security)>show summary

----------------------------------------------------------------------
Secu Policy Name      Authen      Encryption      Associated WLANs
----------------------------------------------------------------------
1 Default             Manual      no encrypt      Lobby
2 WEP Demo            Manual      WEP 64          2nd Floor
3 Open                Manual      no encrypt      1st Floor

WPA Countermeasure    enable
```

Related Commands:

create	Creates security parameters for the specified WLAN.

For information displaying existing WLAN security settings using the applet (GUI), see "Enabling Authentication and Encryption Schemes" on page 200.

AP4700>admin(network.wireless.security)>create

Defines the parameter of access point security policies.

Syntax

create						Defines the parameters of a security policy.
	show					Displays new or existing security policy parameters.
	set	sec-name	<name>			Sets the name of the security policy.
		auth	<authtype>			Sets the authentication type for WLAN <idx> to <type> (none, eap, or kerberos).
						Note: Kerberos parameters are only in affect if "kerberos" is specified for the authentication method (set auth <type>).
		kerb	realm	<name>		Sets the Kerberos realm.
			server	<sidx>	<ip>	Sets the Kerberos server <sidx> (1-primary, 2-backup, or 3-remote) to KDC IP address.
			port	<sidx>	<port>	Sets the Kerberos port to <port> (KDC port) for server <ksidx> (1-primary, 2-backup, or 3-remote).
						Note: EAP parameters are only in affect if "eap" is specified for the authentication method (set auth <type>).
		eap	server	<sidx>	<ip>	Sets the RADIUS server (1-primary or as 2-secondary) IP address <ip>.
			port	<sidx>	<port>	Sets the RADIUS server <sidx> (1-primary or 2-secondary) <port> (1-65535).
			secret	<sidx>	<secret>	Sets the EAP shared secret <secret> (1-63 characters) for server <sidx> (1-primary or 2-secondary).
			reauth	mode	<mode>	Enables or disables EAP reauthentication.
				period	<time>	Sets the reauthentication period <period> in seconds (30-9999).
				retry	<number>	Sets the maximum number of reauthentication retries <retry> (1-99).
			accounting	mode	<mode>	Enable or disable RADIUS accounting.
				server	<ip>	Set external RADIUS server IP address.
				port	<port>	Set external RADIUS server port number.

		secret	<secret>	Set external RADIUS server shared secret password.
		timeout	<period>	Defines MU timout period in seconds (1-255).
		retry	<number>	Sets the maximum number of MU retries to <retry> (1-10).
		syslog	<mode>	Enable or disable syslog messages.
		ip	<ip>	Defines syslog server IP address.
	adv	mu-quiet	<time>	Set the EAP MU/supplicant quiet period to <time> seconds (1-65535).
		mu-timeout	<timeout>	Sets the EAP MU/supplicant timeout in seconds (1-255).
		mu-tx	<time>	Sets the EAP MU/supplicant TX period <time> in seconds (1-65535).
		mu-retry	<count>	Sets the EAP maximum number of MU retries to <count> (1-10).
		svr-timeout	<time>	Sets the server timeout <time> in seconds (1-255).
		svr-retry	<count>	Sets the maximum number of server retries to <count> (1-255).
				Note: The WEP authentication mechanism saves up to four different keys (one for each WLAN). It is not requirement to set all keys, but you must associate a WLAN with the same keys.
enc	<idx>	<type>		Sets the encryption type to <type> (one of none, wep40, wep104, keyguard, tkip, or ccmp) for WLAN <idx>.
wep-keyguard	passkey	<passkey>		The passkey used as a text abbreviation for the entire key length (4-32).
	index	<key index>		Selects the WEP/KeyGuard key (from one of the four potential values of <key index> (1-4).
	hex-key	<kidx>	<key string>	Sets the WEP/KeyGuard key for key index <kidx> (1-4) for WLAN <kidx> to <key string>.
	ascii-key	<kidx>	<key string>	Sets the WEP/KeyGuard key for key index <kidx> (1-4) for WLAN <kidx> to <key string>.
	mixed-mode	<mode>		Enables or disables interoperation with WEP128 clients.
				Note: TKIP parameters are only affected if "tkip" is selected as the encryption type.

	tkip	rotate-mode	<mode>	Enables or disabled the broadcast key.
		interval	<time>	Sets the broadcast key rotation interval to <time> in seconds (300-604800).
		allow-wpa2-tkip	<mode>	Enables or disables the interoperation with wpa2-tkip clients.
		preauth	<mode>	Enables or disables preauthentication (fast roaming).
		opp-pmk-caching		Enables or disables opportunistic PMK.
		ptk-timeout	<time>	Sets the PTK timeout in milliseconds (1-100).
		ptk-retry	<count>	Sets the PTK retry count (1-10).
		type	<key type>	Sets the TKIP key type.
		key	<256 bit key>	Sets the TKIP key to <256 bit key>.
		phrase	<ascii phrase>	Sets the TKIP ASCII pass phrase to <ascii phrase> (8-63 characters).
	ccmp	rotate-mode	<mode>	Enables or disabled the broadcast key.
		interval	<time>	Sets the broadcast key rotation interval to <time> in seconds (300-604800).
		type	<key type>	Sets the CCMP key type.
		phrase	<ascii phrase>	Sets the CCMP ASCII pass phrase to <ascii phrase> (8-63 characters).
		key	<256 bit key>	Sets the CCMP key to <256 bit key>.
		mixed-mode-with-tkip	<mode>	Enables or disables mixed mode (allowing WPA-TKIP clients).
		mixed-mode-with-wep	<mode>	Enables or disables mixed mode (allowing WPA-WEP clients).
		preauth	<mode>	Enables or disables preauthentication (fast roaming).
		opp-pmk-caching		Enables or disables opportunistic PMK.
		ptk-timeout	<time>	Sets the PTK timeout in milliseconds (1-100).
		ptk-retry	<count>	Sets the PTK retry count (1-10).
add-policy				Adds the policy and exits.
..				Disregards the policy creation and exits the CLI session.

For information on configuring the encryption and authentication options available to the access point using the applet (GUI), see "Configuring Security Options" on page 197.

AP4700>admin(network.wireless.security.edit)>

Edits the properties of a specific security policy.

Syntax

show		Displays the new or modified security policy parameters.
set	<index>	Edits security policy parameters. The values subject to modification, are the same ones created using the "AP4700>admin(network.wireless.security)>create" command.
change		Completes policy changes and exits the session.
..		Cancels the changes made and exits the session.

Example

```
admin(network.wireless.security)>edit 1
admin(network.wireless.security.edit)>show

Policy Name                        : Default
Authentication type                : Manual Pre-shared key/No Authentication

Encryption type                    : no encryption
```

For information on configuring the encryption and authentication options available to the access point using the applet (GUI), see "Configuring Security Options" on page 197.

AP4700>admin(network.wireless.security)>delete

Deletes a specific security policy.

Syntax

delete	<sec-name>	Removes the specified security policy from the list of supported policies.
	<all>	Removes all security policies except the default policy.

For information on configuring the encryption and authentication options available to the access point using the applet (GUI), see "Configuring Security Options" on page 197.

Network ACL Commands

AP4700>admin(network.wireless.acl)>

Displays the access point Mobile Unit *Access Control List* (ACL) submenu. The items available under this command include:

show	Displays the access point's current ACL configuration.
create	Creates an MU ACL policy.
edit	Edits the properties of an existing MU ACL policy.
delete	Removes an MU ACL policy.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless.acl)>show

Displays the access point's current ACL configuration.

Syntax

show	summary		Displays the list of existing MU ACL policies.
	policy	<index>	Displays the requested MU ACL index policy.

Example

```
admin(network.wireless.acl)>show summary
----------------------------------------------------------------------
ACL Policy Name            Associated WLANs
----------------------------------------------------------------------
1 Default                  Front Lobby, WLAN1
2 Admin                    Administration
3 Demo Room                Customers

admin(network.wireless.acl)>show policy 1

Policy Name                       : Default
Policy Mode                       : allow

-----------------------------------------------------------------------------
index                  start mac                  end mac
-----------------------------------------------------------------------------
1                      00A0F8348787               00A0F8348798
```

For information on configuring the ACL options available to the access point using the applet (GUI), see "Configuring a WLAN Access Control List (ACL)" on page 153.

AP4700>admin(network.wireless.acl)>create

Creates an MU ACL policy.

Syntax

create	show		<acl-name>	Displays the parameters of a new ACL policy.
	set	acl-name	<index>	Sets the MU ACL policy name.
		mode	<acl-mode>	Sets the ACL mode for the defined index (1-16). Allowed MUs can access the access point managed LAN. Options are deny and allow.
	add-addr	<mac1> or <mac1> <mac2>		Adds specified MAC address to list of ACL MAC addresses.
	delete	<index>	<all>	Removes either a specified ACL index or all ACL entries.
	add-policy			Completes the policy creation and exits the CLI.
	..			Cancels the creation of the ACL and exits the CLI.

Example

```
admin(network.wireless.acl.create)>show

Policy Name                         : Front Lobby
Policy Mode                         : allow

-----------------------------------------------------------------------------
index                    start mac                     end mac
-----------------------------------------------------------------------------
1                        00A0F8334455                  00A0F8334455
2                        00A0F8400000                  00A0F8402001


admin(network.wireless.acl.create)>set acl-name engineering
admin(network.wireless.acl.create)>set mode deny
admin(network.wireless.acl.create)>add-addr 00A0F843AABB
admin(network.wireless.acl.create)>add-policy
```

For information on configuring the ACL options available to the access point using the applet (GUI), see “Configuring a WLAN Access Control List (ACL)” on page 153.

AP4700>admin(network.wireless.acl.edit)>

Edits the properties of an existing MU ACL policy.

Syntax

show	Displays MU ACL policy and its parameters.
set	Modifies the properties of an existing MU ACL policy.
add-addr	Adds an MU ACL table entry.
delete	Deletes an MU ACL table entry, including starting and ending MAC address ranges.
change	Completes the changes made and exits the session.
..	Cancels the changes made and exits the session.

For information on configuring the ACL options available to the access point using the applet (GUI), see "Configuring a WLAN Access Control List (ACL)" on page 153.

AP4700>admin(network.wireless.acl)>delete

Removes an MU ACL policy.

Syntax

delete	<name>	Deletes a partilcular MU ACL policy.
	all	Deletes all MU ACL policies.

For information on configuring the ACL options available to the access point using the applet (GUI), see "Configuring a WLAN Access Control List (ACL)" on page 153.

Network Radio Configuration Commands

AP4700>admin(network.wireless.radio)>

Displays the access point Radio submenu. The items available under this command include:

show	Summarizes access point radio parameters at a high-level.
set	Defines the access point radio configuration.
radio1	Displays the 2.4 GHz radio submenu.
radio2	Displays the 5.0 GHz radio submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless.radio)>show

Displays the access point's current radio configuration.

Syntax

show	Displays the access point's current radio configuration.

Example

```
admin(network.wireless.radio)>show

Radio Configuration

Radio 1
Name                                    : Radio 1
Radio Mode                              : enable
Radio Function                          : WLAN
RF Band of Operation                    : 802.11n(2.4 GHz)
Maximum MUs                             : 127

Wireless AP Configuration:
  Base Bridge Mode                      : enable
  Max Wireless AP Clients               : 6
  Client Bridge Mode                    : disable
  Roaming Client Bridge Mode            : disable
  Client Bridge WLAN                    : WLAN1
  Mesh Connection Timeout               : enable

Radio 2
Name                                    : Radio 2
Radio Mode                              : enable
Radio Function                          : WIPS
RF Band of Operation                    : 802.11n(5 GHz)
Roaming Client Bridge Mode              : disabled

Wireless Mesh Configuration:
  Base Bridge Mode                      : enable
  Max Wireless Mesh ients               : 5
  Client Bridge Mode                    : disable
  Roaming Client Bridge Mode            : enable
  Client Bridge WLAN                    : WLAN1
  Mesh Connection Timeout               : enable

Dot11 Auth Algorithm                    : open-system-only

Radio 3
Name                                    : Radio 3
Radio Mode                              : enable
Radio Function                          : WIPS

Dot11 Auth Algorithm                    : open-system-only

DSCP QoS Mappings                       :
DSCP Values                             :
```

For information on configuring the Radio Configuration options available to the access point using the applet (GUI), see "Setting the WLAN's Radio Configuration" on page 169.

AP4700>admin(network.wireless.radio)>set

Sets the access point's radio configuration and defines the RF band of operation.

Syntax

set	radio-config	<mode>	Sets the radio configuration. The options available differ depending on the single, dual or three radio configuration deployed (see examples below).
	max-mus	<mus>>	Defines the maximum number of MUs assigned to the specified radio (idx 1 or 2). The range can be defined between 0 and 127. This command does not apply to single radio access points.
	mesh-base	<mode>	Enables or disables base bridge mode.
	mesh-max	<clients>	Sets the maximum number of wireless bridge clients.
	mesh-client	<mode>	Enables or Disables client bridge mode.
	mesh-roaming-client	<mode>	Enables or disables the mesh roaming client mode. For information on the Mesh Roaming Client feature, see "Mesh Roaming Client" on page 25.
	mesh-timeout	<mode>	Sets the client bridge link timeout.
	mesh-wlan	<name>	Defines the client bridge WLAN name.
	dot11-auth	<auth-algorithm>	Defines dot11 level authentication algorithm to either open-system-only or shared-key-allowed.
	qos-mapping (wired-to-wireless)	<mode>	Sets the QoS mapping from wired to wireless.

Example

```
admin(network.wireless.radio)>set max-mus 127
admin(network.wireless.radio)>set mesh-base 1 enable
admin(network.wireless.radio)>set mesh-max 1 11
admin(network.wireless.radio)>set mesh-client 1 disable
admin(network.wireless.radio)>set mesh-roaming-client 1 enable
admin(network.wireless.radio)>set mesh-wlan wlan1
admin(network.wireless.radio)>set dot11-auth shared-key-allowed
```

CAUTION

A 40 MHz channel is composed of two 20 MHz subchannels. If the firmware detects radar within the FCC 80 % detection band of the 40 MHz channel; the device must vacate the channel. If the detected signal falls outside the FCC 80 % detection band of one of the 20 MHz subchannels; the Master Device can legally move to that 20 MHz channel.

Three Radio SKU

set	radio-config	<value 1-8>		
			1	Radio 1 WLAN, Radio 2 WLAN, Radio 3 WIPS
			2	Radio 1 WLAN, Radio 2 WIPS, Radio 3 WIPS
			3	Radio 1 WIPS, Radio 2 WLAN, Radio 3 WIPS
			4	Radio 1 WLAN, Radio 2 WLAN, Radio 3 Disabled
			5	Radio 1 WIPS, Radio 2 WIPS, Radio 3 Disabled
			6	Radio 1 WLAN, Radio 2 Disabled, Radio 3 Disabled

			7	Radio 1 Disabled, Radio 2 WLAN, Radio 3 Disabled
			8	Radio 1 Disabled, Radio 2 Disabled, Radio 3 Disabled

Two Radio SKU

set	radio-config	<value 1-7>		
			1	Radio 1 WLAN, Radio 2 WIPS
			2	Radio 1 WIPS, Radio 2 WLAN
			3	Radio 1 WLAN, Radio 2 WLAN
			4	Radio 1 WIPS, Radio 2 WIPS
			5	Radio 1 WLAN, Radio 2 Disabled
			6	Radio 1 Disabled, Radio 2 WLAN
			7	Radio 1 Disabled, Radio 2 Disabled

Single Radio SKU

set	radio-config	<value 1-4>		
			1	Radio 1 WIPS
			2	Radio 1 WLAN (B/G/N)
			3	Radio 1 WLAN (A/N)
			4	Radio 1 Disabled

NOTE

For legacy (pre 4.1) deployments, imported radio configurations are supported (with the exception of the removed (11a, 11b, wips-radio and rf-function) commands. However, the configuration export operation only exports the radio-config (1-8).

For information on the options available to the access point, see “Setting the WLAN’s Radio Configuration” on page 169.

AP4700>admin(network.wireless.radio.802-11n[2.4 GHz])>

Displays a specific 802.11n 2.4 GHz radio 1 submenu. The items available under this command include:

Syntax

```
show                                : show 802.11n radio parameters
set                                 : set 802.11n radio parameters
delete                              : delete 802.11n radio parameters
                                    :
advanced                            : go to Advanced Settings sub-menu
mesh                                : go to Mesh Connections sub-menu
                                    :
..                                  : go to parent menu
/                                   : go to root menu
                                    :
save                                : save cfg to system flash
quit                                : quit cli
```

For information on configuring Radio 1 Configuration options available to the access point using the applet (GUI), see "Setting the WLAN's Radio Configuration" on page 169.

AP4700>admin(network.wireless.radio.802-11n[2.4 GHz])>show

Displays specific 802.11n (2.4 GHz) radio settings.

Syntax

show	radio	Displays specific 802.11n (2.4 GHz) radio settings.
	rates	Displays specific 802.11n (2.4 GHz) radio rate settings.
	aggr	Displays specific 802.11n (2.4 GHz) aggregation settings.
	qos	Displays specific 802.11n (2.4 GHz) radio WMM QoS settings.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz])>show radio

Radio Setting Information

Placement                         : indoor
MAC Address                       : 00A0F8715920
Radio Type                        : 802.11n (2.4 GHz)
ERP Protection                    : Off
HT Protection Mode                : Pure HT

Channel Setting                   : user selection
Power Level                       : 5 dbm (4 mW)

802.11 rate compatibility mode    : B, G, and N

Beacon Interval                   : 100 K-usec
DTIM Interval                     : 10 beacon intvls

short preamble                    : disable
RTS Threshold                     : 2341 bytes

QBSS Channel Util Beacon Intervl  : 10 beacon intvls
QBSS Load Element Mode            : enable

Single Anetenna                   : disable
Dynamic Chain Selection           : disable
TKIP HT rates compatibility       : disable
Current BCMC-Tx-Speed for         : range optimization

admin(network.wireless.radio.802-11n[2.4 GHz])>show rates

802.11 rate configuration:
Basic Rates              1 2 5.5 11
Supported Rates          1 2 5.5 6 9 11 12 18 24 36 48 54
Short Guard Interval     disable
-----------------------------------------------------------------------------
MCS Index      Basic/Supported     20 MHz Rate     40 MHz Rate
-----------------------------------------------------------------------------
0              Supported            6.5 Mbps       13.5 Mbps
1              Supported           13.0 Mbps       27.0 Mbps
2              Supported           19.5 Mbps       40.5 Mbps
3              Supported           26.0 Mbps       54.0 Mbps
```

```
4              Supported           39.0 Mbps       81.0 Mbps
5              Supported           52.0 Mbps       108.0 Mbps
6              Supported           58.5 Mbps       121.5 Mbps
7              Supported           65.0 Mbps       135.0 Mbps
8              Supported           13.0 Mbps       27.0 Mbps
9              Supported           26.0 Mbps       54.0 Mbps
10             Supported           39.0 Mbps       81.0 Mbps
11             Supported           52.0 Mbps       108.0 Mbps
12             Supported           78.0 Mbps       162.0 Mbps
13             Supported          104.0 Mbps       216.0 Mbps
14             Supported          117.0 Mbps       243.0 Mbps
15             Supported          130.0 Mbps       270.0 Mbps

admin(network.wireless.radio.802-11n[2.4 GHz])>

admin(network.wireless.radio.802-11n[2.4 GHz])>show aggr

Radio Aggregation Settings
Receive A-MSDU Buffer Limit             :3839 bytes

Enable Transmit A-MPDU                  :enable
Transmit A-MPDU Size Limit              :65536 bytes
Receive A-MPDU Size Limit               :65536 bytes
Receive A-MPDU Minimum Spacing          :0 usec

admin(network.wireless.radio.802-11n[2.4 GHz])>

admin(network.wireless.radio.802-11n[2.4 GHz])>show qos

Radio QOS Parameter Set              11n-default
-----------------------------------------------------------------------------
Access Category      CWMin      CWMax      AIFSN      TXOPs (32 usec) TXOPs ms
-----------------------------------------------------------------------------
Background           15         1023       7          0               0.000
Best Effort          15         63         3          31              0.992
Video                7          15         1          94              3.008
Voice                3          7          1          47              1.504
```

CAUTION

If you do NOT include the index number (for example, "set dtim 50"), the DTIMs for all four BSSIDs will be changed to 50. To change individual DTIMs for BSSIDs, specify the BSS Index number (for example, "set dtim 2 50). This will change the DTIM for BSSID 2 to 50.

For information on configuring the Radio 1 Configuration options available to the access point using the applet (GUI), see “Configuring a WLAN Access Control List (ACL)” on page 153.

AP4700>admin(network.wireless.radio.802-11n[2.4 GHz])>set

Defines specific 802.11n (2.4 GHz) radio parameters.

Syntax

set	placement	Defines the access point radio placement as indoors or outdoors.
	ch-mode	Determines how the radio channel is selected (user, auto-20 or auto-40).
	channel	Defines the radio channel used. Channel allowed depends on actual country of operation.
	power	Defines the antenna power transmit level. Depends on radio type, channel and country.
	antenna-type	Sets the numerical antenna type used with the access point (0-7). Antenna types include: 0-Default antenna, 1-Dual band antenna, 2-Omni antenna, 3-Yagi antenna, 4-Embedded antenna, 5-Panel antenna, 6-Patch antenna, 7-Sector antenna.
	antenna-gain	Sets the gain used by the selected antenna type (between 0.00 - 30.00 dBm)
	rf-mode	Sets the default rates for the 802.11 mode selected (b-only, g-only, n-only, b-and-g, or bg-and-n).
	rates	Sets the supported radio transmit rates.
	beacon	Sets the beacon interval used by the radio.
	dtim	Defines the DTIM interval (by index) used by the radio.
	aggr	Sets the radio’s aggregation.
	shortgi	Enables/disables a short guard interval of 40MHz.
	preamble	Enables/disables short preamble support for the radio (this is 2.4 GHz radio specific).
	rts	Defines the RTS Threshold value for the radio.
	range	Sets the radio’s extended range (in miles 0-50).
	qos	Defines the cwmin, cwmax, aifsn and txops levels for the QoS policy used for the radio.
	qbss-beacon	Sets the QBSS Channel Util Beacon Interval in kilo-usec (10 - 200).
	qbss-mode	Enables/disables the QBSS load element.
	single-antenna	Enables/disables single antenna support. Enable (default setting) to decrease sensitivity and device retries.
	dynamic-chain-selection	Enables/disables dynamic chain selection for the radio. For more information, see “Dynamic Chain Selection” on page 20.
	tkip-ht-compatibility	Enables/disables TKIP-HT rates compatibility.
	bcmc-tx-speed	Sets the transmission speed to either range or throughout mode.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz])>set placement indoor
admin(network.wireless.radio.802-11n[2.4 GHz])>set ch-mode user
admin(network.wireless.radio.802-11n[2.4 GHz])>set channel 11
admin(network.wireless.radio.802-11n[2.4 GHz])>set power 4
admin(network.wireless.radio.802-11n[2.4 GHz])>set antenna-type 1
admin(network.wireless.radio.802-11n[2.4 GHz])>set antenna-gain 10.00
admin(network.wireless.radio.802-11n[2.4 GHz])>set rf-mode b-only
admin(network.wireless.radio.802-11n[2.4 GHz])>set rates
admin(network.wireless.radio.802-11n[2.4 GHz])>set beacon 100
admin(network.wireless.radio.802-11n[2.4 GHz])>set dtim 1 40
admin(network.wireless.radio.802-11n[2.4 GHz])>set aggr ampdu enable
admin(network.wireless.radio.802-11n[2.4 GHz])>set shortgi disable
admin(network.wireless.radio.802-11n[2.4 GHz])>set single-antenna disable
admin(network.wireless.radio.802-11n[2.4 GHz])>set preamble disable
admin(network.wireless.radio.802-11n[2.4 GHz])>set rts 2341
admin(network.wireless.radio.802-11n[2.4 GHz])>set qos cwmin 125
admin(network.wireless.radio.802-11n[2.4 GHz])>set qos cwmax 255
admin(network.wireless.radio.802-11n[2.4 GHz])>set qos aifsn 7
admin(network.wireless.radio.802-11n[2.4 GHz])>set qos txops 0
admin(network.wireless.radio.802-11n[2.4 GHz])>set qbss-beacon 110
admin(network.wireless.radio.802-11n[2.4 GHz])>set qbss-mode enable
admin(network.wireless.radio.802-11n[2.4 GHz])>set dynamic-chain-selection enable
admin(network.wireless.radio.802-11n[2.4 GHz])>set tkip-ht-compatibility disable
admin(network.wireless.radio.802-11n[2.4 GHz])>set bcmc-tx-speed range
```

For information on configuring the Radio 1 Configuration options available to the access point using the applet (GUI), see “Configuring the 802.11a/n or 802.11b/g/n Radio” on page 174.

AP4700>admin(network.wireless.radio.802-11n[2.4 GHz].advanced)>

Displays the advanced submenu for the 802.11n (2.4 GHz) radio. The items available under this command include:

Syntax

show	Displays advanced radio settings for the 802.11n (2.4 GHz) radio.
set	Defines advanced parameters for the 802.11n (2.4 GHz) radio.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless.radio.802-11n[2.4 GHz].advanced)> show

Displays the BSSID to WLAN mapping for the 802.11n (2.4 GHz) radio.

Syntax

show	advanced	Displays advanced settings for the 802.11n (2.4 GHz) radio.
	wlan	Displays WLAN summary list for the 802.11n (2.4 GHz) radio.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz].advanced)>show advanced

------------------------------------------------------------------------------
      WLAN      BSS ID      BC/MC Cipher       Status      Message
------------------------------------------------------------------------------

      Lobby     1           Open               good        configuration is ok
      HR        2           Open               good        configuration is ok
      Office    3           Open               good        configuration is ok

------------------------------------------------------------------------------
      BSSID      Primary WLAN
------------------------------------------------------------------------------

      1          Lobby
      2          HR
      3          Office

admin(network.wireless.radio.802-11n[2.4 GHz].advanced)>show wlan

WLAN 1:
WLAN name                        : WLAN1
ESS ID                           : 101
Radio Band(s)                    : 2.4 and 5.0 GHz
VLAN                             : <none>
Security Policy                  : Default
QoS Policy                       : Default
Rate Limiting                    : disabled
```

For information on configuring Radio 1 Configuration options available to the access point using the applet (GUI), see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174.

AP4700>admin(network.wireless.radio.802-11n[2.4 GHz].advanced)>set

Defines advanced parameters for the target 802.11n (2.4 GHz) radio.

Syntax

set	wlan	<wlan-name>	<bssid>	Defines advanced WLAN to BSSID mapping for the target radio.
	bss	<bss-id>	<wlan name>	Sets the BSSID to primary WLAN definition.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz].advanced)>set wlan demoroom 1
admin(network.wireless.radio.802-11n[2.4 GHz].advanced)>set bss 1 demoroom
```

For information on configuring Radio 1 Configuration options available to the access point using the applet (GUI), see “Configuring the 802.11a/n or 802.11b/g/n Radio” on page 174.

AP4700>admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>

Displays the mesh configuration submenu for the 802.11n (2.4 GHz) radio. The items available under this command include:

Syntax

show	Displays mesh settings and status for the 802.11n (2.4 GHz) radio.
set	Defines mesh parameters for the 802.11n (2.4 GHz) radio.
add	Adds a 802.11n (2.4 GHz) radio mesh connection.
delete	Deletes a 802.11n (2.4 GHz) radio mesh connection.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>show

Displays mesh settings and status for the 802.11n (2.4 GHz) radio.

Syntax

show	config	Displays the connection list configuration.
	status	Shows the available mesh connection status.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>show config

Mesh Connection Auto Select                    : enable

admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>show status
-----------------------------------------------------------------------------
idx      AP MAC Address     Channel     Signal (dBm)
-----------------------------------------------------------------------------

admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>
```

AP4700>admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>set

Defines mesh parameters for the 802.11n (2.4 GHz) radio.

Syntax

set	<auto-select>	Enables or disables auto select mesh connections.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>set auto-select enable
admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>show config

Mesh Connection Auto Select                    : enable
```

AP4700>admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>add

Adds a 802.11n (2.4 GHz) radio mesh connection.

Syntax

add	<priority>	Defines the connection priority (1-16).
	<mac>	Sets the access point MAC address.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>add 2 AA21DCDD12DE
```

AP4700>admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>delete

Deletes a 802.11n (2.4 GHz) radio mesh connection by specified index or by removing all entries.

Syntax

delete	<idx>	Deletes a mesh connection by specified index (1-16).
	<all>	Removes all mesh connections.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>delete 2
```

AP4700>admin(network.wireless.radio.802-11n[5.0 GHz])>

Displays a specific 802.11n (5.0 GHz) radio 2 submenu.

The items available under this command include:

Syntax

```
  show                            : show 802.11n radio parameters
  set                             : set 802.11n radio parameters
  delete                          : delete 802.11n radio parameters
                                  :
  advanced                        : go to Advanced Settings sub-menu
  mesh                            : go to Mesh Connections sub-menu
                                  :
  ..                              : go to parent menu
  /                               : go to root menu
                                  :
  save                            : save cfg to system flash
  quit                            : quit cli
```

AP4700>admin(network.wireless.radio.802-11n[5.0 GHz])>show

Displays specific 802.11n (5.0 GHz) radio settings.

Syntax

show	radio	Displays specific 802.11n (5.0 GHz) radio settings.
	rates	Displays specific 802.11n (5.0 GHz) radio rate settings.
	aggr	Displays specific 802.11n (5.0 GHz) aggregation settings.
	qos	Displays specific 802.11n (5.0 GHz) radio WMM QoS settings.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz])>show radio

Radio Setting Information

Placement                         : indoor
MAC Address                       : 00A0F8715920
Radio Type                        : 802.11n (5.0 GHz)
HT Protection Mode                : Pure HT

Channel Setting                   : uniform spreading
Power Level                       : 20 dbm (100 mW)

802.11 rate compatibility mode    : A and N

Beacon Interval                   : 100 K-usec
DTIM Interval                     : 10 beacon intvls

RTS Threshold                     : 2341 bytes

QBSS Channel Util Beacon Intervl  : 10 beacon intvls
QBSS Load Element Mode            : enable

Single Antenna                    : disable
Dynamic Chain Selection           : disable
TKIP HT rates compatibility       : disable
Current BCMC-Tx-Speed for         : range optimization
admin(network.wireless.radio.802-11n[5.0 GHz])>show rates

Basic Rates              6 12 24
Supported Rates          6 9 12 18 24 36 48 54
Short Guard Interval     disable
-----------------------------------------------------------------------------
MCS Index      Basic/Supported     20 MHz Rate     40 MHz Rate
-----------------------------------------------------------------------------
0              Supported            6.5 Mbps       13.5 Mbps
1              Supported           13.0 Mbps       27.0 Mbps
2              Supported           19.5 Mbps       40.5 Mbps
3              Supported           26.0 Mbps       54.0 Mbps
4              Supported           39.0 Mbps       81.0 Mbps
5              Supported           52.0 Mbps       108.0 Mbps
6              Supported           58.5 Mbps       121.5 Mbps
7              Supported           65.0 Mbps       135.0 Mbps
```

```
8              Supported           13.0 Mbps       27.0 Mbps
9              Supported           26.0 Mbps       54.0 Mbps
10             Supported           39.0 Mbps       81.0 Mbps
11             Supported           52.0 Mbps       108.0 Mbps
12             Supported           78.0 Mbps       162.0 Mbps
13             Supported          104.0 Mbps       216.0 Mbps
14             Supported          117.0 Mbps       243.0 Mbps
15             Supported          130.0 Mbps       270.0 Mbps

admin(network.wireless.radio.802-11n[5.0 GHz])>

admin(network.wireless.radio.802-11n[5.0 GHz])>show aggr

Radio Aggregation Settings
Enable Transmit A-MSDU                  :enable
Transmit A-MSDU Buffer Limit            :3839 bytes

Enable Transmit A-MPDU                  :enable
Transmit A-MPDU Size Limit              :65536 bytes
Receive A-MPDU Size Limit               :65536 bytes
Receive A-MPDU Minimum Spacing          :0 usec

admin(network.wireless.radio.802-11n[5.0 GHz])>

admin(network.wireless.radio.802-11n[5.0 GHz])>show qos

Radio QOS Parameter Set              11n-default
-----------------------------------------------------------------------------
Access Category      CWMin      CWMax      AIFSN      TXOPs (32 usec) TXOPs ms
-----------------------------------------------------------------------------
Background           15         1023       7          0               0.000
Best Effort          15         63         3          31              0.992
Video                7          15         1          94              3.008
Voice                3          7          1          47              1.504
```

For information on configuring the Radio 2 Configuration options available to the access point using the applet (GUI), see “Configuring a WLAN Access Control List (ACL)” on page 153.

AP4700>admin(network.wireless.radio.802-11n[5.0 GHz])>set

Defines specific 802.11n (5.0 GHz) radio parameters.

Syntax

set	placement	Defines the access point radio placement as indoors or outdoors.
	ch-mode	Determines how the radio channel is selected.
	channel	Defines the actual channel used by the radio. Channel allowed depends on actual country of operation.
	power	Defines the antenna power transmit level. Depends on radio type, channel and country.
	antenna-type	Sets the numerical antenna type used with the access point (0-7). Antenna types include: 0-default antenna, 1-dual band antenna, 2-Omni antenna, 3-Yagi antenna, 4-Embedded antenna, 5-Panel antenna, 6-Patch antenna, 7-Sector antenna.
	antenna-gain	Sets the gain used by the selected antenna type (between 0.00 - 30.00 dBm)
	rf-mode	Sets the default rates for the 802.11 mode selected (a-only, n-only, or a-and-n).
	rates	Sets the supported radio transmit rates.
	beacon	Sets the beacon interval used by the radio.
	dtim	Defines the DTIM interval (by index) used by the radio.
	aggr	Sets the radio's aggregation.
	shortgi	Enables/disables a short guard interval of 40MHz.
	rts	Defines the RTS Threshold value for the radio.
	range	Sets the radio's extended range (in miles 0-50).
	qos	Defines the param-set, cwmin, cwmax, aifsn and txops levels for the QoS policy used for the 5.0 GHz radio.
	qbss-beacon	Sets the QBSS Channel Util Beacon Interval in kilo-usec (10 - 200).
	qbss-mode	Enables/disables the QBSS load element.
	single-antenna	Enables/disables single antenna support. Enable (default setting) to decrease sensitivity and device retries.
	dynamic-chain-selection	Enables/disables dynamic chain selection for the radio. For more information, see "Dynamic Chain Selection" on page 20.
	tkip-ht-compatibility	Enables/disables TKIP-HT rates compatibility.
	bcmc-tx-speed	Sets the transmission speed to either range or throughout mode.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz])>

admin(network.wireless.radio.802-11n[5.0 GHz])>set placement indoor
admin(network.wireless.radio.802-11n[5.0 GHz])>set ch-mode auto-40
admin(network.wireless.radio.802-11n[5.0 GHz])>set channel 11
admin(network.wireless.radio.802-11n[5.0 GHz])>set antenna-type 2
admin(network.wireless.radio.802-11n[5.0 GHz])>set antenna-gain 10.00
admin(network.wireless.radio.802-11n[5.0 GHz])>set power 4
admin(network.wireless.radio.802-11n[5.0 GHz])>set rates 10
admin(network.wireless.radio.802-11n[5.0 GHz])>set beacon 100
admin(network.wireless.radio.802-11n[5.0 GHz])>set dtim 1 10
admin(network.wireless.radio.802-11n[2.4 GHz])>set aggr ampdu enable
admin(network.wireless.radio.802-11n[2.4 GHz])>set shortgi disable
admin(network.wireless.radio.802-11n[5.0 GHz])>set rts 2341
admin(network.wireless.radio.802-11n[5.0 GHz])>set range 40
admin(network.wireless.radio.802-11n[5.0 GHz])>set qbss-beacon 110
admin(network.wireless.radio.802-11n[5.0 GHz])>set qbss-mode enable
admin(network.wireless.radio.802-11n[5.0 GHz])>set single-antenna disable
admin(network.wireless.radio.802-11n[5.0 GHz])>set dynamic-chain-selection enable
admin(network.wireless.radio.802-11n[5.0 GHz])>set tkip-ht-compatibility disable
admin(network.wireless.radio.802-11n[5.0 GHz])>set bcmc-tx-speed range
```

CAUTION

A 40 MHz channel is composed of two 20 MHz subchannels. If the firmware detects radar within the FCC 80 % detection band of the 40 MHz channel; the device must vacate the channel. If the detected signal falls outside the FCC 80 % detection band of one of the 20 MHz subchannels; the Master Device can legally move to that 20 MHz channel.

For information on configuring the Radio 2 Configuration options available to the access point using the applet (GUI), see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174.

AP4700>admin(network.wireless.radio.802-11n[5.0 GHz].advanced)>

Displays the advanced submenu for the 802.11n (5.0 GHz) radio.

The items available under this command include:

Syntax

show	Displays advanced radio settings for the 802.11n (5.0 GHz) radio.
set	Defines advanced parameters for the 802.11n (5.0 GHz) radio.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless.radio.802-11n[5.0 GHz].advanced)> show

Displays the BSSID to WLAN mapping for the 802.11n (5.0 GHz) radio.

Syntax

show	advanced	Displays advanced settings for the 802.11n (5.0 GHz) radio.
	wlan	Displays WLAN summary list for 802.11n (5.0 GHz) radio.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz].advanced)>show advanced

-----------------------------------------------------------------------------
      WLAN      BSS ID      BC/MC Cipher      Status      Message
-----------------------------------------------------------------------------

      Lobby     1           Open              good        configuration is ok
      HR        2           Open              good        configuration is ok
      Office    3           Open              good        configuration is ok

-----------------------------------------------------------------------------
      BSSID      Primary WLAN
-----------------------------------------------------------------------------

      1          Lobby
      2          HR
      3          Office

admin(network.wireless.radio.802-11n[5.0 GHz].advanced)>show wlan

WLAN 1:
WLAN name                      : WLAN1
ESS ID                         : 101
Radio                          : 2.4 and 5.0 GHz
VLAN                           : <none>
Security Policy                : Default
QoS Policy                     : Default
Rate Limiting                  : disable
```

For information on configuring the Radio 2 Configuration options available to the access point using the applet (GUI), see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174.

AP4700>admin(network.wireless.radio.802-11n[5.0 GHz].advanced)> set

Defines advanced parameters for the target 802.11n (5.0 GHz) radio.

Syntax

set	wlan	<wlan-name>	<bssid>	Defines advanced WLAN to BSSID mapping for the target 5.0 GHz radio.
	bss	<bss-id>	<wlan name>	Sets the BSSID to primary WLAN definition.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz].advanced)>set wlan demoroom 1
admin(network.wireless.radio.802-11n[5.0 GHz].advanced)>set bss 1 demoroom
```

For information on configuring Radio 2 Configuration options available to the access point using the applet (GUI), see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174.

AP4700>admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>

Displays the mesh configuration submenu for the 802.11n (5.0 GHz) radio.

The items available under this command include:

Syntax

show	Displays mesh settings and status for the 802.11n (5.0 GHz) radio.
set	Defines mesh parameters for the 802.11n (5.0 GHz) radio.
add	Adds a 802.11n (5.0 GHz) radio mesh connection.
delete	Deletes a 802.11n (5.0 GHz) radio mesh connection.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>show

Displays mesh settings and status for the 802.11n (5.0 GHz) radio.

Syntax

show	config	Displays the connection list configuration.
	status	Shows the available mesh connection status.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>show config

Mesh Connection Auto Select                  : enable

admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>show status
-----------------------------------------------------------------------------
idx      AP MAC Address     Channel     Signal (dBm)
-----------------------------------------------------------------------------

admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>
```

AP4700>admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>set

Defines mesh parameters for the 802.11n (5.0 GHz) radio.

Syntax

set	<auto-select>	Enables or disables auto select mesh connections.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>set auto-select enable
admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>show config

Mesh Connection Auto Select                    : enable
```

AP4700>admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>add

Adds a 802.11n (5.0 GHz) radio mesh connection.

Syntax

add	<priority>	Defines the connection priority (1-16).
	<mac>	Sets the access point MAC address.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>add 2 AA21DCDD12DE
```

AP4700>admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>delete

Deletes a 802.11n (5.0 GHz) radio mesh connection by specified index or by removing all entries.

Syntax

delete	<idx>	Deletes a mesh connection by specified index (1-16).
	<all>	Removes all mesh connections.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>delete 2
```

Network Quality of Service (QoS) Commands

AP4700>admin(network.wireless.qos)>

Displays the access point *Quality of Service* (QoS) submenu. The items available under this command include:

show	Displays access point QoS policy information.
create	Defines the parameters of the QoS policy.
edit	Edits the settings of an existing QoS policy.
delete	Removes an existing QoS policy.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless.qos)>show

Displays the access point’s current QoS policy by summary or individual policy.

Syntax

show	summary		Displays all exisiting QoS policies that have been defined.
	policy	<index>	Displays the configuration for the requested QoS policy.

Example

```
admin(network.wireless.qos)>show summary

----------------------------------------------------------------------
QOS Policy Name            Associated WLANs
----------------------------------------------------------------------
1 Default                  WLAN1, mudskipper
2 IP Phones                Audio Dept
3 Video                    Vidio Dept

admin(network.wireless.qos)>show policy 1

Policy Name                        Default
Support Voice Prioritization       disable
Multicast (Mask) Address 1         01005E000000
Multicast (Mask) Address 2         09000E000000
WMM QOS Mode                       disable
WMM QOS Parameter Set              11ag-default
```

For information on configuring the WLAN QoS options available to the access point using the applet (GUI), see “Setting the WLAN Quality of Service (QoS) Policy” on page 156.

AP4700>admin(network.wireless.qos.create)>

Defines an access point QoS policy.

Syntax

show				Displays QoS policy parameters.
set	qos-name	<index>		Sets the QoS name for the specified index entry.
	vop	<index>		Enables or disables support (by index) for legacy VOIP devices.
	mcast	<mac>		Defines primary and secondary Multicast MAC address.
	wmm-qos	<index>		Enables or disables the QoS policy index specified.
	param-set	<set-name>		Defines the data type used with the qos policy and mesh network. When set to a value other then manual, editing the access category values is not necessary. Options include; 11g-default, 11b-default, 11g-wifi, 11b-wifi, 11g-voice, 11b-voice or manual for advanced users).
	cwmin	<access category>	<index>	Defines Minimum Contention Window (CW-Min) for specified access categoiry and index.
	cwmax	<access category>	<index>	Defines Maximum Contention Window (CW-Max) for specified access categoiry and index.
	aifsn	<access category>	<index>	Sets Arbitrary Inter-Frame Space Number (AIFSN) for specified access categoiry and index.
	txops	<access category>	<index>	Configures Opportunity to Transmit Time (TXOPs Time) for specified access categoiry and index.
	default		<index>	Defines CWMIN, CWMAX, AIFSN and TXOPs default values.
add-policy				Completes the policy edit and exits the session.
..				Cancels the changes and exits.

For information on configuring the WLAN QoS options available to the access point using the applet (GUI), see "Setting the WLAN Quality of Service (QoS) Policy" on page 156.

AP4700>admin(network.wireless.qos.edit)>

Edits the properties of an existing QoS policy.

Syntax

show				Displays QoS policy parameters.
set	qos-name	<index>		Sets the QoS name for the specified index entry.
	vop	<index>		Enables or disables support (by index) for legacy VOIP devices.
	mcast	<mac>		Defines primary and secondary Multicast MAC address.
	wmm-qos	<index>		Enables or disables the QoS policy index specified.
	param-set	<set-name>		Defines the data type used with the qos policy and mesh network. When set to a value other then manual, editing the access category values is not necessary. Options include; 11g-default, 11b-default, 11g-wifi, 11b-wifi, 11g-voice, 11b-voice or manual for advanced users).
	cwmin	<access category>	<index>	Defines the Minimum Contention Window (CW-Min) for specified access categoiry and index.
	cwmax	<access category>	<index>	Defines the Maximum Contention Window (CW-Max) for specified access categoiry and index.
	aifsn	<access category>	<index>	Sets the Arbitrary Inter-Frame Space Number (AIFSN) for specified access categoiry and index.
	txops	<access category>	<index>	Configures Opportunity to Transmit Time (TXOPs Time) for specified access categoiry and index.
	default		<index>	Defines CWMIN, CWMAX, AIFSN and TXOPs default values.
change				Completes the policy edit and exits the session.
..				Cancels the changes and exits.

For information on configuring the WLAN QoS options available to the access point using the applet (GUI), see "Setting the WLAN Quality of Service (QoS) Policy" on page 156.

AP4700>admin(network.wireless.qos)>delete

Removes a QoS policy.

Syntax

delete	<qos-name> <all>	Deletes the specified QoS polciy index, or all of the policies (except default policy).

For information on configuring the WLAN QoS options available to the access point using the applet (GUI), see "Setting the WLAN Quality of Service (QoS) Policy" on page 156.

Network Rate Limiting Commands

AP4700>admin(network.wireless.rate-limiting)>

Displays the access point Rate Limiting submenu. The items available under this command include:

show	Displays Rate Limiting information for how data is processed by the access point.
set	Defines Rate Limiting parameters for the access point.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless.rate-limiting)>show

Displays the access point's current Rate Limiting configuration.

Syntax

show	summary wlan	Displays the current Rate Limiting configuration for defined WLANs.

Example

```
admin(network.wireless.rate-limiting>show summary

Per MU Rate Limiting               : disable

admin(network.wireless.rate-limiting)>show wlan

WLAN 1
WLAN Name                   WLAN1
ESSID                       101
Radio Band(s)               2.4 and 5.0 GHz
VLAN                        <none>
Security Policy             Default
QoS Policy                  Default
Rate Limiting               disable
```

For information on configuring the Rate Limiting options available to the access point using the applet (GUI), see "Configuring MU Rate Limiting" on page 184.

AP4700>admin(network.wireless.rate-limiting)>set

Defines the access point Rate Limiting configuration.

Syntax

set	mode	<mode>	Enables or disables Rate Limiting.

For information on configuring the Rate Limiting options available to the access point using the applet (GUI), see “Configuring MU Rate Limiting” on page 184.

Network Rogue-AP Commands

AP4700>admin(network.wireless.rogue-ap)>

Displays the Rogue AP submenu. The items available under this command include:

show	Displays the current access point Rogue AP detection configuration.
set	Defines the Rogue AP detection method.
mu-scan	Goes to the Rogue AP mu-uscan submenu.
allowed-list	Goes to the Rogue AP Allowed List submenu.
active-list	Goes the Rogue AP Active List submenu.
rogue-list	Goes the Rogue AP List submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless.rogue-ap)>show

Displays the current access point Rogue AP detection configuration.

Syntax

show	Displays the current access point Rogue AP detection configuration.

Example

```
admin(network.wireless.rogue-ap)>show

MU Scan                           : disable
MU Scan Interval                  : 60 minutes
On-Channel                        : disable
Detector Radio Scan               : enable

Auto Authorize Extreme APs       : disable

Approved APs age out              : 0 minutes
Rogue APs age out                 : 0 minutes
```

For information on configuring the Rogue AP options available to the access point using the applet (GUI), see “Configuring Rogue AP Detection” on page 243.

AP4700>admin(network.wireless.rogue-ap)>set

Defines the access point ACL rogue AP method.

Syntax

```
set
   mu-scan                           : enable/disable MU Scan
   interval                          : set MU Scan interval
   on-channel                        : enable/disable On Channel Detection
   detector-scan                     : enable/disable AP Detector Scan
   ABG-scan                          : enable/disable Detector Scan on Both Bands
                                     : (2.4 & 5.0 GHz)
   extreme networks-ap               : enable/disable Authorization of Any AP
                                     : having Extreme Networks Defined MAC Addresses
                                     :
   applst-ageout                     : set the approved AP age out time
   roglst-ageout                     : set the rogue AP age out time
```

Example

```
admin(network.wireless.rogue-ap)>

admin(network.wireless.rogue-ap)>set mu-scan enable
admin(network.wireless.rogue-ap)>set interval 10
admin(network.wireless.rogue-ap)>set on-channel disable
admin(network.wireless.rogue-ap)>set detector-scan disable
admin(network.wireless.rogue-ap)>set ABG-scan disable
admin(network.wireless.rogue-ap)>set extreme-ap enable
admin(network.wireless.rogue-ap)>set applst-ageout 10
admin(network.wireless.rogue-ap)>set roglst-ageout 10

admin(network.wireless.rogue-ap)>show

MU Scan                            : enable
MU Scan Interval                   : 10 minutes
On Channel                         : disable
Detector Radio Scan                : disable

Auto Authorize Extreme APs       : enable

Approved AP age out                : 10 minutes
Rogue AP age out                   : 10 minutes
```

For information on configuring the Rogue AP options available to the access point using the applet (GUI), see “Configuring Rogue AP Detection” on page 243.

AP4700>admin(network.wireless.rogue-ap.mu-scan)>

Displays the Rogue-AP mu-scan submenu.

Syntax

add	Add all or just one scan result to Allowed AP list.
show	Displays all APs located by the MU scan.
start	The access point initiates an immediate scan for known and associated MUs.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless.rogue-ap.mu-scan)>start

Initiates an MU scan from a user provided MAC address.

Syntax

start	<mu-mac>	Initiates MU scan from user provided MAC address.

For information on configuring the Rogue AP options available to the access point using the applet (GUI), see “Configuring Rogue AP Detection” on page 243.

AP4700>admin(network.wireless.rogue-ap.mu-scan)>show

Displays the results of an MU scan.

Syntax

show	Displays all APs located by the MU scan.

For information on configuring the Rogue AP options available to the access point using the applet (GUI), see “Configuring Rogue AP Detection” on page 243.

AP4700>admin(network.wireless.rogue-ap.allowed-list)>

Displays the Rogue-AP allowed-list submenu.

show	Displays the rogue AP allowed list
add	Adds an AP MAC address and ESSID to the allowed list.
delete	Deletes an entry or all entries from the allowed list.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless.rogue-ap.allowed-list)>show

Displays the Rogue AP allowed List.

Syntax

show	Displays the rogue-AP allowed list.

Example

```
admin(network.wireless.rogue-ap.allowed-list)>show

            Allowed AP List
------------------------------------------------------------------------------
index            ap mac             essid
------------------------------------------------------------------------------

1          00:A0:F8:71:59:20        *
2          00:A0:F8:33:44:55        101
3          00:A0:F8:40:20:01        Marketing
```

For information on configuring the Rogue AP options available to the access point using the applet (GUI), see “Configuring Rogue AP Detection” on page 243.

AP4700>admin(network.wireless.rogue-ap.allowed-list)>add

Adds an AP MAC address and ESSID to existing allowed list.

Syntax

add	<mac-addr> <ess-id>	Adds an AP MAC address and ESSID to existing allowed list. “ffffffffffffffff” means any MAC Use a “*” for any ESSID.

Example

```
admin(network.wireless.rogue-ap.allowed-list)>add 00A0F83161BB 103
admin(network.wireless.rogue-ap.allowed-list)>show

------------------------------------------------------------------------------
index            ap                 essid
------------------------------------------------------------------------------

1          00:A0:F8:71:59:20        *
2          00:A0:F8:33:44:55        fffffffffff
3          00:A0:F8:40:20:01        Marketing
4          00:A0:F8:31:61:BB        103
```

For information on configuring the Rogue AP options available to the access point using the applet (GUI), see “Configuring Rogue AP Detection” on page 243.

AP4700>admin(network.wireless.rogue-ap.allowed-list)>delete

Deletes an AP MAC address and ESSID to existing allowed list.

Syntax

delete	<idx> (1-50) <all>	Deletes an AP MAC address and ESSID (or all addresses) from the allowed list.

For information on configuring the Rogue AP options available to the access point using the applet (GUI), see "Configuring Rogue AP Detection" on page 243.

WIPS Commands

AP4700>admin(network.wireless.wips)>

Displays the WIPS submenu. The items available under this command include:

show	Displays the current WLAN Intrusion Prevention configuration.
set	Sets WLAN Intrusion Prevention parameters.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless.wips)>show

Shows the WLAN Intrusion Prevention configuration.

Syntax

show	Displays the existing Wireless Intrusion Protection System (WIPS) configuration.

Example

```
admin(network.wireless.wips>show

WIPS Server #1
   IP Address               : 192.168.0.21

WIPS Server #2
   IP Address               : 10.1.1.1

admin(network.wireless.wips>
```

AP4700>admin(network.wireless.wips)>set

Sets the WLAN Intrusion Prevention configuration.

Syntax

set	<idx 1 and 2> <ip>	Defines the WLAN Intrusion Prevention Server IP Address (for server IPs 1 and 2).

Example

```
admin(network.wireless.wips)>set server 1 192.168.0.21
admin(network.wireless.wips)>
```

Network MU Locationing Commands

AP4700>admin(network.wireless.mu-locationing)>

Displays the MU Locationing submenu.

The items available under this command include:

show	Displays the current MU Locationing configuration.
set	Defines MU Locationing parameters.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.wireless.mu-locationing)>show

Displays the MU probe table configuration.

Syntax

show	Displays the MU locationing probe table configuration.

Example

```
admin(network.wireless.mu-locationing)>show

MU Probe Table Mode               : disable
MU Probe Table Size               : 200

admin(network.wireless.mu-locationing)>
```

AP4700>admin(network.wireless.mu-locationing>set

Defines the MU probe table configuration used for locating MUs.

Syntax

set		Defines the MU probe table configuration.
	mode	Enables/disables MU locationing.
	size	Defines the number of MUs in the locationing table (the maximum allowed is 200).

Example

```
admin(network.wireless.mu-locationing)>set

admin(network.wireless.mu-locationing)>set mode enable
admin(network.wireless.mu-locationing)>set size 200

admin(network.wireless.mu-locationing)>
```

Network Firewall Commands

AP4700>admin(network.firewall)>

Displays the access point firewall submenu.

The items available under this command include:

show	Displays the access point’s current firewall configuration.
set	Defines the access point’s firewall parameters.
access	Enables/disables firewall permissions through the LAN and WAN ports.
advanced	Displays interoperaility rules between the LAN and WAN ports.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.firewall)>show

Displays the access point firewall parameters.

Syntax

show	Shows all access point firewall settings.

Example

```
admin(network.firewall)>show

Firewall Status                    : disable
NAT Timeout                        : 10 minutes

Configurable Firewall Filters:

ftp bounce attack filter           : enable
syn flood attack filter            : enable
unaligned ip timestamp filter      : enable
source routing attack filter       : enable
winnuke attack filter              : enable
seq num prediction attack filter   : enable
mime flood attack filter           : enable
max mime header length             : 8192 bytes
max mime headers                   : 16 headers
```

For information on configuring the Firewall options available to the access point using the applet (GUI), see "Configuring Firewall Settings" on page 218.

AP4700>admin(network.firewall)>set

Defines the access point firewall parameters.

Syntax

set	mode	<mode>	Enables or disables the firewall.
	nat-timeout	<interval>	Defines the NAT timeout value.
	syn	<mode>	Enables or disables SYN flood attack check.
	src	<mode>	Enables or disables source routing check.
	win	<mode>	Enables or disables Winnuke attack check.
	ftp	<mode>	Enables or disables FTP bounce attack check.
	ip	<mode>	Enables or disables IP unaligned timestamp check.
	seq	<mode>	Enables or disables sequence number prediction check.
	mime	filter	Enables or disables MIME flood attack check.
	len	<length>	Sets the max header length in bytes as specified by <length> (with value in range 256 - 34463).
	hdr	<count>	Sets the max number of headers as specified in <count> (with value in range 12 - 34463).

Example

```
admin(network.firewall)>set mode enable
admin(network.firewall)>set ftp enable
admin(network.firewall)>set ip enable
admin(network.firewall)>set seq enable
admin(network.firewall)>set src enable
admin(network.firewall)>set syn enable
admin(network.firewall)>set win enable
admin(network.firewall)>show

Firewall Status                   : enable
Override LAN to WAN Access        : disable

Configurable Firewall Filters

ftp bounce attack filter          : enable
syn flood attack filter           : enable
unaligned ip timestamp filter     : enable
source routing attack filter      : enable
winnuke attack filter             : enable
seq num prediction attack filter  : enable
mime flood attack filter          : enable
max mime header length            : 8192
max mime headers                  : 16
```

AP4700>admin(network.firewall)>access

Enables or disables firewall permissions through LAN to WAN ports.

Syntax

show	Displays LAN to WAN access rules.
set	Sets LAN to WAN access rules.
add	Adds LAN to WAN exception rules.
delete	Deletes LAN to WAN access exception rules.
list	Displays LAN to WAN access exception rules. for the specified LAN.
..	Goes to parent menu
/	Goes to root menu.
save	Saves configuration to system flash.
quit	Quits and exits the CLI session.

Example

```
admin(network.firewall.lan-wan-access)>list lan1

-----------------------------------------------------------------------------
index      from      to      name      prot      start port      end port
-----------------------------------------------------------------------------

1          lan       wan     HTTP      tcp       80              80
2          lan       wan     abc       udp        0              0
3          lan       wan     123456    ah        1440            2048
4          lan       wan     654321    tcp       2048            2048
5          lan       wan     abc       ah        100             1000
```

For information on configuring the Firewall options available to the access point using the applet (GUI), see “Configuring Firewall Settings” on page 218.

AP4700>admin(network.firewall)>advanced

Displays whether an access point firewall rule is intended for inbound traffic to an interface or outbound traffic from that interface.

Syntax

show	Shows advanced subnet access parameters.
set	Sets advanced subnet access parameters.
import	Imports rules from subnet access.
inbound	Goes to the Inbound Firewall Rules submenu.
outbound	Goes to the Outbound Firewall Rules submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to flash memory.
quit	Quits and exits the CLI session.

Example

```
admin(network.firewall.adv-lan-access)>inbound
admin(network.firewall.adv-lan-access.inb)>list
-----------------------------------------------------------------------------
Idx  SCR IP-Netmask  Dst IP-Netmask  TP  SPorts  DPorts  Rev  NAT  Action
-----------------------------------------------------------------------------
1    1.2.3.4         2.2.2.2         all 1:      1:      0.0.0.0   deny
     255.0.0.0       255.0.0.0           65535   65535   nat port 33
2    33.3.0.0        10.10.1.1       tcp 1:      1:      11.11.1.0 allow
     255.255.255.0   255.255.255.0       65535   65535   nat port 0
```

For information on configuring the Firewall options available to the access point using the applet (GUI), see "Configuring Firewall Settings" on page 218.

Network Router Commands

AP4700>admin(network.router)>

Displays the router submenu. The items available under this command are:

show	Displays the existing access point router configuration.
set	Sets the RIP parameters.
add	Adds user-defined routes.
delete	Deletes user-defined routes.
list	Lists user-defined routes.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.router)>show

Shows the access point route table.

Syntax

show	rip	Displays the rounter's RIP parameters.
	routes	Displays connected routes.

Example

```
admin(network.router)>show rip
rip type                          : off
rip direction                     : both
rip authentication type           : none
rip simple auth password          : *********
rip md5 id 1                      : 1
rip md5 key 1                     : *********
rip md5 id 2                      : 1
rip md5 key 2                     : *********

admin(network.router)>show routes
----------------------------------------------------------------------------
index  destination      netmask          gateway          interface   metric
----------------------------------------------------------------------------
1      192.168.2.0      255.255.255.0    0.0.0.0          lan1        0
2      192.168.1.0      255.255.255.0    0.0.0.0          lan2        0
3      192.168.0.0      255.255.255.0    0.0.0.0          lan1        0
4      192.168.24.0     255.255.255.0    0.0.0.0          wan         0
5      157.235.19.5     255.255.255.0    192.168.24.1     wan         1

Default gateway Interface: wan
```

For information on configuring the Router options available to the access point using the applet (GUI), see "Configuring Router Settings" on page 186.

AP4700>admin(network.router)>set

Shows the access point route table.

Syntax

set	auth	Sets the RIP authentication type (none, simple or MD5).
	dir	Sets RIP direction (rx, tx or both)
	id	Sets MD5 authetication ID (1-256) for specific index (1-2).
	key	Sets MD5 authetication key (up to 16 characters) for specified inded (1-2).
	passwd	Sets the password (up to 16 characters) for simple authentication.
	type	Defines the RIP type (off, ripv1, ripv2, or ripv1v2).
	dgw-iface	Sets the default gateway interface (lan1, lan2, wan or none).

For information on configuring the Router options available to the access point using the applet (GUI), see “Configuring Router Settings” on page 186.

AP4700>admin(network.router)>add

Adds user-defined routes.

Syntax

add	<dest>	<netmask>	<gw>	<iface>	<metric>	Adds a route with destination IP address <dest>, IP netmask <netmask>, destination gateway IP address <gw>, interface LAN1, LAN2 or WAN <iface>, and metric set <metric> to (1-65536).

Example

```
admin(network.router)>add 192.168.3.0 255.255.255.0 192.168.2.1 LAN1 1

admin(network.router)>list
----------------------------------------------------------------------------
index  destination      netmask          gateway          interface   metric
----------------------------------------------------------------------------
1      192.168.3.0      255.255.255.0  192.168.2.1      lan1        1
```

For information on configuring the Router options available to the access point using the applet (GUI), see "Configuring Router Settings" on page 186.

AP4700>admin(network.router)>delete

Deletes user-defined routes.

Syntax

delete	<idx>	Deletes the user-defined route <idx> (1-20) from list.
	all	Deletes all user-defined routes.

Example

```
admin(network.router)>list
----------------------------------------------------------------------------
index  destination     netmask          gateway          interface   metric
----------------------------------------------------------------------------
1      192.168.2.0     255.255.255.0    192.168.0.1      lan1        1
2      192.168.1.0     255.255.255.0    0.0.0.0          lan2        0
3      192.168.0.0     255.255.255.0    0.0.0.0          lan2        0

admin(network.router)>delete 2
admin(network.router)>list
------------------------------------------------------------------
index destination netmask gateway interface metric
------------------------------------------------------------------
1      192.168.2.0     255.255.255.0    0.0.0.0          lan1        0
2      192.168.0.0     255.255.255.0    0.0.0.0          lan1        0

admin(network.router)>
```

For information on configuring the Router options available to the access point using the applet (GUI), see “Configuring Router Settings” on page 186.

AP4700>admin(network.router)>list

Lists user-defined routes.

Syntax

list	Displays a list of user-defined routes.

Example

```
admin(network.router)>list

----------------------------------------------------------------------------
index  destination      netmask          gateway          interface   metric
----------------------------------------------------------------------------
1      192.168.2.0      255.255.255.0    192.168.0.1      lan1        1
2      192.168.1.0      255.255.255.0    0.0.0.0          lan2        0
3      192.168.0.0      255.255.255.0    0.0.0.0          lan1        0
```

For information on configuring the Router options available to the access point using the applet (GUI), see “Configuring Router Settings” on page 186.

Network IP Filter Commands

AP4700>admin(network.ipfilter)>

Displays the ipfilter submenu. The items available under this command are:

show	Displays Global IP Filter table entries.
set	Sets Global IP Filter table entries.
add	Adds a filter to the Global IP Filter table
delete	Deletes a filter from the Global IP Filter table.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(network.ipfilter)>show

Displays Global IP Filter table entries.

Syntax

show	Displays Global IP Filter table entries.

Example

```
admin(network.ipfilter)>show

----------------------------------------------------------------------------
Idx name  Protocol  Port-Start-End  SrcIP-Start-End  DestIP-Start-End  In-Use
----------------------------------------------------------------------------


admin(network.ipfilter)>
```

AP4700>admin(network.ipfilter)>set

Sets Global IP Filter table entries.

Syntax

set	Sets Global IP Filter table entries.

Example

```
admin(network.ipfilter)>set

name                           : Sets name of IP Filters
protocol                       : Sets the protocol of the IP filter
port-start                     : Sets the starting port of the IP Filter
port-end                       : Sets the end port of the IP Filter
saddr-start                    : Sets the source address start of the IP Filter
saddr-end                      : Sets the source address end of the IP Filter
daddr-start                    : Sets the destination address start of the IP Filter
daddr-end                      : Sets the destination address end of the IP Filter

admin(network.ipfilter)>
```

AP4700>admin(network.ipfilter)>add

Adds a filter to the Global IP Filter table.

Syntax

add	filter-name	<name>	Adds name to IP Filter (up to 20 characters).
	protocol	<loc>	Adds protocol for IP Filter.
	start-port	<port>	Adds a starting port for IP Filter.
	end-port	<port>	Adds an ending port for IP Filter.
	start-src-address	<ip>	Adds a starting source IP address for IP Filter.
	end-src-address	<ip>	Adds an ending source IP address for IP Filter.
	start-dest-address	<ip>	Adds a starting destination IP address for IP Filter.
	end-dest-address	<ip>	Adds an ending destination IP address for IP Filter.

AP4700>admin(network.ipfilter)>delete

Deletes a filter from the Global IP Filter table.

Syntax

delete	index	<idx>	Deletes a filter index from the Global IP Filter table.
	all		Deletes all filters from the Global IP Filter table.

Example

```
admin(network.ipfilter)>delete all
admin(network.ipfilter)>
```

System Commands

AP4700>admin(system)>

Displays the System submenu. The items available under this command are shown below.

restart	Restarts the access point.
show	Shows access point system parameter settings.
set	Defines access point system parameter settings.
lastpw	Displays last debug password.
exec	Goes to a Linux command menu.
arp	Dispalys the access point's arp table.
power-setup	Goes to the Power Settings submenu.
aap-setup	Goes to the Adaptive AP Settings submenu.
lldp	Goes to the LLDP submenu.
access	Goes to the access point access submenu where access point access methods can be enabled.
cmgr	Goes the Certificate Manager submenu.
snmp	Goes to the SNMP submenu.
userdb	Goes to the user database submenu.
RADIUS	Goes to the RADIUS submenu.
ntp	Goes to the Network Time Protocol submenu.
logs	Displays the log file submenu.
config	Goes to the configuration file update submenu.
fw-update	Goes to the firmware update submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(system)>restart

Restarts the access point access point.

Syntax

restart	Restarts the access point.

Example

```
admin(system)>restart

********************************WARNING***********************************
** Unsaved configuration changes will be lost when the access point is reset.
** Please be sure to save changes before resetting.
**************************************************************************

Are you sure you want to restart the AP4700?? (yes/no):

AP4700 Boot Firmware Version 4.1.0.0-xxx

Press escape key to run boot firmware ........

Power On Self Test

testing ram              : pass
testing nor flash        : pass
testing nand flash       : pass
testing ethernet         : pass
```

For information on restarting the access point using the applet (GUI), see "Configuring System Settings" on page 78.

AP4700>admin(system)>show

Displays high-level system information helpful to differentiate this access point.

Syntax

show	Displays access point system information.

Example

```
admin(system)>show

system name                         : AP-00-04-96-54-A0-10
system location                     : AP-00-04-96-54-A0-10-Location
admin email address                 :
system uptime                       : 3 days 23 hours 17 minutes 14 seconds
DNS Relay Mode                      : enable

SSLv2 support from HTTP server      : enable
weak cipher support in SSL          : enable
SSHv1 support                       : enable
led state                           : enable

AP4700 firmware version             : 4.1.1.0-022R
country code                        : us
ap-mode                             : independent
serial number                       : 10289-80867
model                               : AP4750-US
hw version                          : A

admin(system)>
```

For information on displaying System Settings using the applet (GUI), see “Configuring System Settings” on page 78.

AP4700>admin(system)>set

Sets access point system parameters.

Syntax

set	name	<name>	Sets the access point system name to <name> (1 to 59 characters). The access point does not allow intermediate space characters between characters within the system name. For example, “AP4700 sales” must be changed to “AP4700sales” to be a valid system name.
	loc	<loc>	Sets the access point system location to <loc> (1 to 59 characters).
	email	<email>	Sets the access point admin email address to <email> (1 to 59 characters).
	cc	<code>	Sets the access point country code using two letters <code>.
	led	<mode>	Sets the access point’s LED state.
	dns-relay-mode	<mode>	Enables/disables DNS relay to prevent access to the port used by DNS.
	sslv2	<mode>	Enables/disables SSLv2 support for encryption and message authentication.
	weak-ssl-cipher	<mode>	Enables/disables the AP to support SSL ciphers less than 128 bits in length.
	sshv1	<mode>	Enables/disables SSHv1 support for remote connections.

```
admin(system)>set name phils
admin(system)>set loc engineering
admin(system)>set email mudskipper@yahoo.com
admin(system)>set cc us
admin(system)>set sslv2 enable
admin(system)>set weak-ssl-cipher enable
admin(system)>set sshv1 enable
admin(system)>set dns-relay-mode enable
```

NOTE

This name will appear in the WIPS server when one of the radios is configured as a sensor and the WIPS functionality connects to the WIPS server. The WIPS module only accepts names with up to 20 characters, keep that if intending to use this AP as a sensor.

For information on configuring System Settings using the applet (GUI), see “Configuring System Settings” on page 78.

AP4700>admin(system)>lastpw

Displays last expired debug password.

Example

```
admin(system)>lastpw

AP-4700 MAC Address is 00:15:70:02:7A:66
Last debug password was extreme
Current debug password used 0 times, valid 4 more time(s)

admin(system)>
```

AP4700>admin(system)>arp

Dispalys the access point’s arp table.

Example

```
admin(system)>arp

IP Address               HWtype  HWaddress           Flags Mask      Device

157.235.92.210           ether   00:11:25:14:61:A8   C
157.235.92.179           ether   00:14:22:F3:D7:39   C
157.235.92.248           ether   00:11:25:B2:09:60   C
157.235.92.180           ether   00:0D:60:D0:06:90   C
157.235.92.3             ether   00:D0:2B:A0:D4:FC   C
157.235.92.181           ether   00:15:C5:0C:19:27   C
157.235.92.80            ether   00:11:25:B2:0D:06   C
157.235.92.95            ether   00:14:22:F9:12:AD   C
157.235.92.161           ether   00:06:5B:97:BD:6D   C
157.235.92.126           ether   00:11:25:B2:29:64   C

admin(system)>
```

Power Setup Commands

AP4700>admin(system)>power-setup

Displays the Power Setup submenu.

show	Displays the current power setting configuration.
set	Defines the access point’s power setting configuration.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the current configuration to the access point system flash.
quit	Quits the CLI and exits the current session.

For information on configuring power settings using the applet (GUI), see “Configuring Power Settings” on page 81.

AP4700>admin(system.power-setup)>show

Displays the access point's current power configuration.

Syntax

show	Displays the access point's current power configuration.

Example

```
admin(system.power-setup)>show

Power Mode                          : Auto
Power Status                        : Full Power
3af Power Option                    : default
3at Power Option                    : default
Default Radio                       : Radio1
```

For information on configuring power settings using the applet (GUI), see "Configuring Power Settings" on page 81 .

AP4700>admin(system.power-setup)>set

Sets access point's power consumption configuration.

Syntax

set	mode	Sets the power mode to either Auto or 3af. Changing the mode requires restarting the access point.
	power-option	Defines the power option.
	def-radio	Defines the access point's default radio (1-Radio1, 2-Radio2).

```
admin(system.power-setup)>set mode Auto
admin(system.power-setup)>set power-option 3af option
admin(system.power-setup)>set def-radio 1
```

For information on configuring power settings using the applet (GUI), see "Configuring Power Settings" on page 81 .

Adaptive AP Setup Commands

AP4700>admin(system)>aap-setup

Displays the Adaptive AP submenu.

show	Displays Adaptive AP information.
set	Defines the Adaptive AP configuration.
delete	Deletes static controller address assignments.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the current configuration to the access point system flash.
quit	Quits the CLI and exits the current session.

For information on configuring adaptive AP using the applet (GUI), see “Adaptive AP Setup” on page 85.

For an overview of adaptive AP functionality and its implications, see “Adaptive AP Overview” on page 605.

AP4700>admin(system.aap-setup)>show

Displays the access point's Adaptive AP configuration.

Syntax

show	Displays the access point's Adaptive AP configuration.

Example

```
admin(system.aap-setup)>show

Auto Discovery Mode                          : disable
Controller Name                                  : greg
Static IP Port                               : 24576
Static IP Address                            :
IP Address 1                                 : 0.0.0.0
IP Address 2                                 : 0.0.0.0
IP Address 3                                 : 0.0.0.0
IP Address 4                                 : 0.0.0.0
IP Address 5                                 : 0.0.0.0
IP Address 6                                 : 0.0.0.0
IP Address 7                                 : 0.0.0.0
IP Address 8                                 : 0.0.0.0
IP Address 9                                 : 0.0.0.0
IP Address 10                                : 0.0.0.0
IP Address 11                                : 0.0.0.0
IP Address 12                                : 0.0.0.0

Tunnel to Controller                             : disable
AC Keepalive                                 : 5
Load Balancing                               : enable
Inactivity Timeout                           : 60

Current Controller                               : 157.235.22.11
AP Adoption State                            : AAP not adopted

admin(system.aap-setup)>
```

For information on configuring adaptive AP using the applet (GUI), see "Adaptive AP Setup" on page 85.

For an overview of adaptive AP functionality and its implications, see "Adaptive AP Overview" on page 605.

AP4700>admin(system.aap-setup)>set

Sets access point's Adaptive AP configuration.

Syntax

set	auto-discovery	Sets the controller auto-discovery mode (enable/disable).
	ipadr	Defines the controller IP address used.
	name	Defines the controller name for DNS lookups (up to 127 characters).
	port	Sets the port.
	passphrase	Defines the pass phrase or key for controller connection.
	tunnel-to-controller	Enables/disables the tunnel between controller and access point.
	ac-keepalive	Defines the keepalive interval.
	load-balancing	Enables or disables AAP load balancing.

```
admin(system.aap-setup)>set auto-discovery enable
admin(system.aap-setup)>set ipadr 192.235.111.10
admin(system.aap-setup)>set port 1812
admin(system.aap-setup)>set passphrase mudskipper
admin(system.aap-setup)>set load-balancing enable
```

For information on configuring adaptive AP using the applet (GUI), see "Adaptive AP Setup" on page 85.

For an overview of adaptive AP functionality and its implications, see "Adaptive AP Overview" on page 605.

AP4700>admin(system.aap-setup)>delete

Deletes static controller address assignments.

Syntax

delete	<idx>	Deletes static controller address assignments by selected index.
	<all>	Deletes all assignments.

Example

```
admin(system.aap-setup)>delete 1

admin(system.aap-setup)>
```

For information on configuring Adaptive AP using the applet (GUI), see "Adaptive AP Setup" on page 85.

For an overview of adaptive AP functionality and its implications, see "Adaptive AP Overview" on page 605.

LLDP Commands

AP4700>admin(system)>lldp

Displays the LLDP submenu.

show	Displays LLDP information.
set	Sets LLDP parameters.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the current configuration to the access point system flash.
quit	Quits the CLI and exits the current session.

For information on configuring LLDP using the applet (GUI), see "Configuring LLDP Settings" on page 108.

AP4700>admin(system.lldp)>show

Displays LLDP information.

Syntax

show	Displays LLDP information.

```
admin(system.lldp)>show
LLDP Status                      :enable
LLDP Refresh Interval            :30
LLDP Holdtime Mutiplier          :4
admin(system.lldp)>
```

For information on configuring LLDP using the applet (GUI), see “Configuring LLDP Settings” on page 108.

AP4700>admin(system.lldp)>set

Sets the LLDP configuration.

Syntax

set		Sets the LLDP configurarion.
	lldp-mode	Sets AP lldp mode.
	lldp-refresh	Sets the LLDP Refresh Interval.
	lldp-holdtime	Sets the LLDP HoldTime Multiplier.

```
admin(system.lldp)>set lldp-mode enable
admin(system.lldp)>set lldp-refresh 100
admin(system.lldp)>set lldp-holdtime 2
admin(system.lldp)>
```

For information on configuring LLDP using the applet (GUI), see "Configuring LLDP Settings" on page 108.

System Access Commands

AP4700>admin(system)>access

Displays the access point access submenu.

show	Displays access point system access capabilities.
set	Goes to the access point system access submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the current configuration to the access point system flash.
quit	Quits the CLI and exits the current session.

AP4700>admin(system.access)>set

Defines the permissions to access the access point applet, CLI, SNMP as well as defining their timeout values.

Syntax

set	applet		Defines the applet HTTP/HTTPS access parameters.
	app-timeout	<minutes>	Sets the applet timeout. Default is 300 Mins.
	sslv2	<mode>	Enables/disables SSL v2 support.
	cli		Defines CLI Telnet access parameters. Enables/disables access from lan and wan.
	ssh		Sets the CLI SSH access parameters.
	auth-timout	<seconds>	Disables the radio interface if no data activity is detected after the interval defined. Default is 120 seconds.
	inactive-timeout	<minutes>	Inactivity interval resulting in the AP terminating its connection. Default is 120 minutes.
	snmp		Sets SNMP access parameters for the AP's LAN and WAN ports.
	admin-auth		Designates a RADIUS server is used in the authentication verification.
	server	<ip>	Specifies the IP address the Remote Dial-In User Service (RADIUS) server.
	port	<port#>	Specifies the port on which the RADIUS server is listening. Default is 1812.
	secret	<pw>	Defines the shared secret password for RADIUS server authentication (up to 31 characters).
	mode	<mode>	Enables/disables the access point message mode.
	msg		Defines the access point login message text (up to 511 characters).

For information on configuring access point access settings using the applet (GUI), see "Configuring Data Access" on page 87.

AP4700>admin(system.access)>show

Displays the current access point access permissions and timeout values.

Syntax

show	Shows all of the current system access settings for the access point.

Example

```
admin(system.access)>show

-------------------------------From LAN1-------From LAN2-------From WAN
applet http access               enable          enable          enable
applet http access               enable          enable          enable
cli telnet access                enable          enable          enable
cli ssh access                   enable          enable          enable
snmp access                      enable          enable          enable

SSLV2                                        : enable

http/s timeout                               : 0
ssh server authetnication timeout            : 120
ssh server inactivity timeout                : 120
admin authetnication mode                    : local
Login Message Mode                           : disable
Login Message                                :
```

Related Commands:

set	Defines the access point system access capabilities and timeout values.

For information on configuring access point access settings using the applet (GUI), see "Configuring Data Access" on page 87.

System Certificate Management Commands

AP4700>admin(system)>cmgr

Displays the Certificate Manager submenu. The items available under this command include:

genreq	Generates a Certificate Request.
delself	Deletes a Self Certificate.
loadself	Loads a Self Certificate signed by CA.
listself	Lists the self certificate loaded.
loadca	Loads trusted certificate from CA.
delca	Deletes the trusted certificate.
listca	Lists the trusted certificate loaded.
showreq	Displays a certificate request in PEM format.
delprivkey	Deletes the private key.
listprivkey	Lists names of private keys.
expcert	Exports the certificaqte file.
impcert	Imports the certificate file.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(system.cmgr)>genreq

Generates a certificate request.

Syntax

genreq	<IDname >	<Subject>	[-ou <OrgUnit>]	[-on <OrgName>]	[-cn <City>]	[-st <State>]	. . .
	. . .	[-p <PostCode>]	[-cc <CCode>]	[-e <Email>]	[-d <Domain>]	[-i <IP>]	[-sa <SAlgo>]

Generates a self-certificate request for a Certification Authority (CA), where:

<IDname>	The private key ID Name (up to 7 chars)
<Subject>	Subject Name (up to 49 chars)
-ou	Organization Unit (up to 49 chars)
<Department>	Organization Name (up to 49 chars)
-on	City Name of Organization (up to 49 chars)
<OrgName>	State Name (up to 49 chars)
-cn <City>	Postal code (9 digits)
-st <State>	Country code (2 chars)
-p <PostCode>	E-mail Address (up to 49 chars)
-cc <CCode>	Domain Name (up to 49 chars)
-e <Email>	IP Address (a.b.c.d)
-d <Domain>	Signature Algorithm (MD5-RSA or SHA1-RSA)
-i <IP>	Key size in bits (512, 1024, or 2048)
-sa <SAlgo>	
-k <KSize>	

NOTE

The parameters in [square brackets] are optional. Check with the CA to determine what fields are necessary. For example, most CAs require an email address and an IP address, but not the address of the organization.

Example

```
admin(system.cmgr)>genreq MyCert2 MySubject -ou MyDept -on MyCompany

Please wait. It may take some time...
Generating the certificate request
Retreiving the certificate request
The certificate request is
-----BEGIN CERTIFICATE REQUEST-----
MIHzMIGeAgEAMDkxEjAQBgNVBAoTCU15Q29tcGFueTEPMA0GA1UECxMGTXlEZXB0
MRIwEAYDVQQDEwlNeVN1YmplY3QwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAtKcX
plKFCFAJymTFX71yuxY1fdS7UEhKjBsH7pdqnJnsASK6ZQGAqerjpKScWV1mzYn4
1q2+mgGnCvaZUlIo7wIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCClQ5LHdbG/C1f
Bj8AszttSo/bA4dcX3vHvhhJcmuuWO9LHS2imPA3xhX/d6+Q1SMbs+tG4RP0lRSr
iWDyuvwx
-----END CERTIFICATE REQUEST-----
```

For information on configuring certificate management settings using the applet (GUI), see "Managing Certificate Authority (CA) Certificates" on page 91.

AP4700>admin(system.cmgr)>delself

Deletes a self certificate.

Syntax

delself	<IDname>	Deletes the self certificate named <IDname>.

Example

```
admin(system.cmgr)>delself MyCert2
```

For information on configuring self certificate settings using the applet (GUI), see "Creating Self Certificates for Accessing the VPN" on page 92.

AP4700>admin(system.cmgr)>loadself

Loads a self certificate signed by the Certificate Authority.

Syntax

loadself	<IDname>	Load the self certificate signed by the CA with name <IDname> (7 characters).

For information on configuring self certificate settings using the applet (GUI), see "Creating Self Certificates for Accessing the VPN" on page 92.

AP4700>admin(system.cmgr)>listself

Lists the loaded self certificates.

Syntax

listself	Lists all self certificates that are loaded.

For information on configuring self certificate settings using the applet (GUI), see "Creating Self Certificates for Accessing the VPN" on page 92.

AP4700>admin(system.cmgr)>loadca

Loads a trusted certificate from the Certificate Authority.

Syntax

loadca	Loads the trusted certificate (in PEM format) that is pasted into the command line.

For information on configuring certificate settings using the applet (GUI), see "Importing a CA Certificate" on page 91.

AP4700>admin(system.cmgr)>delca

Deletes a trusted certificate.

Syntax

delca	<IDname>	Deletes the trusted certificate.

For information on configuring certificate settings using the applet (GUI), see "Importing a CA Certificate" on page 91.

AP4700>admin(system.cmgr)>listca

Lists the loaded trusted certificate.

Syntax

listca	Lists the loaded trusted certificates.

For information on configuring certificate settings using the applet (GUI), see "Importing a CA Certificate" on page 91.

AP4700>admin(system.cmgr)>showreq

Displays a certificate request in PEM format.

Syntax

showreq	<IDname>	Displays a certificate request named <IDname> generated from the genreq command.

For information on configuring certificate settings using the applet (GUI), see "Importing a CA Certificate" on page 91.

AP4700>admin(system.cmgr)>delprivkey

Deletes a private key.

Syntax

delprivkey	<IDname>	Deletes private key named <IDname>.

For information on configuring certificate settings using the applet (GUI), see "Creating Self Certificates for Accessing the VPN" on page 92.

AP4700>admin(system.cmgr)>listprivkey

Lists the names of private keys.

Syntax

listprivkey	Lists all private keys and displays their certificate associations.

For information on configuring certificate settings using the applet (GUI), see “Importing a CA Certificate” on page 91.

AP4700>admin(system.cmgr)>expcert

Exports the certificate file to a user defined location.

Syntax

expcert	Exports the access point's CA or Self certificate file.

To export certificate information from an Altitude 4700 access point:

```
admin(system.cmgr)>expcert ?

<type> <file name> <cr>             : type: ftp/tftp
                                    : file name: Certificate file name
                                    : Server options for this file are the same
                                    : as that for the configuration file

admin(system.cmgr)>expcert tftp AP-71x1certs.txt
```

To configue certificate management settings while conducting a firmware update or restoring a factory default configuratrion:

```
admin(system.cmgr)> ?

genreq                              : generate a certificate request
delself                             : deletes a signed certificate
loadself                            : loads a signed cerfticiate signed by the CA
listself                            : lists the loaded signed self certificate
loadca                              : loads the root CA certificate
delca                               : deletes the root CA certificate
listca                              : lists the loaded root CA certificate
showreq                             : displays certificate request in PEM format
delprivkey                          : deletes the private key
listprivkey                         : lists the names of the private keys
expcert                             : exports the target cerfticate file
impcert                             : imports the target cerfticate file
(..)                                : goes to the parent menu
/                                   : goes to the root menu
save                                : saves the configuration to system flash
quit                                : quits the CLI session
```

For information on configuring certificate settings using the applet (GUI), see "Importing a CA Certificate" on page 91.

AP4700>admin(system.cmgr)>impcert

Imports the target certificate file.

Syntax

impcert	Imports the target certificate file.

To import certificate information from an Altitude 4700 Access Point:

```
admin(system.cmgr)>impcert ?

<type> <file name> <cr>             : type: ftp/tftp
                                    : file name: Certificate file name
                                    : Server options for this file are the same
                                    : as that for the configuration file

admin(system.cmgr)>impcert tftp AP-4700certs.txt
```

To configue certificate management settings while conducting a firmware update or restoring a factory default configuratrion:

```
admin(system.cmgr)> ?

genreq                              : generate a certificate request
delself                             : deletes a signed certificate
loadself                            : loads a signed certficiate signed by the CA
listself                            : lists the loaded signed self certificate
loadca                              : loads the root CA certificate
delca                               : deletes the root CA certificate
listca                              : lists the loaded root CA certificate
showreq                             : displays certificate request in PEM format
delprivkey                          : deletes the private key
listprivkey                         : lists the names of the private keys
expcert                             : exports the target certficate file
impcert                             : imports the target certficate file
(..)                                : goes to the parent menu
/                                   : goes to the root menu
save                                : saves the configuration to system flash
quit                               : quits the CLI session
```

For information on configuring certificate settings using the applet (GUI), see “Importing a CA Certificate” on page 91.

System SNMP Commands

AP4700>admin(system)> snmp

Displays the SNMP submenu. The items available under this command are shown below.

access	Goes to the SNMP access submenu.
traps	Goes to the SNMP traps submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

System SNMP Access Commands

AP4700>admin(system.snmp.access)

Displays the SNMP Access menu. The items available under this command are shown below.

show	Shows SNMP v3 engine ID.
add	Adds SNMP access entries.
delete	Deletes SNMP access entries.
list	Lists SNMP access entries.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(system.snmp.access)>show

Shows the SNMP v3 engine ID.

Syntax

show	eid	Shows the SNMP v3 Engine ID.

Example

```
admin(system.snmp.access)>show eid

AP4700 snmp v3 engine id          : 000001846B8B4567F871AC68

admin(system.snmp.access)>
```

For information on configuring SNMP access settings using the applet (GUI), see "Configuring SNMP Access Control" on page 101.

AP4700>admin(system.snmp.access)>add

Adds SNMP access entries for specific v1v2 and v3 user definitions.

Syntax

add	acl	<ip1>	<ip2>	Adds an entry to the SNMP access control list with <ip1> as the starting IP address and <ip2> and as the ending IP address.	
	v1v2c	<comm>	<access>	<oid>	
				: comm - community string 1 to 31 characters	
				: access - read/write access - (ro,rw)	
				: oid - string 1 to 127 chars - E.g. 1.3.6.1	
	v3	<user>	<access>	<oid>	<sec>
		<auth>	<pass1>	<priv>	<pass2>
				: user - username 1 to 31 characters	
				: access - read/write access - (ro,rw)	
				: oid - string 1 to 127 chars - E.g. 1.3.6.1	
				: sec - security - (none,auth,auth/priv)	
				: auth - algorithm - (md5,sha1)	
				: *(required only if sec is - auth,auth/priv)*	
				: pass1 - auth password - 8 to 31 chars	
				: *(required only if sec is 'auth,auth/priv')*	
				: priv - algorithm - (des, aes)	
				: *(required only if sec is 'auth/priv')*	
				: pass2 - privacy password - 8 to 31 chars	
				: (required only if sec is 'auth/priv')	
				The following parameters must be specified if <sec> is not none: Authentication type <auth> set to md5 or sha1 Authentication password <pass1> (8 to 31 chars)	
				The following parameters must be specified if <sec> is set to auth/priv: Privacy algorithm set to des or aes Privacy password <pass2> (8 to 31 chars)	

For information on configuring SNMP access settings using the applet (GUI), see "Configuring SNMP Access Control" on page 101.

AP4700>admin(system.snmp.access)>delete

Deletes SNMP access entries for specific v1v2 and v3 user definitions.

Syntax

delete	acl	<idx>	Deletes entry <idx> (1-10) from the access control list.
		all	Deletes all entries from the access control list.
	v1v2c	<idx>	Deletes entry <idx> (1-10) from the v1/v2 configuration list.
		all	Deletes all entries from the v1/v2 configuration list.
	v3	<idx>	Deletes entry <idx> (1-10) from the v3 user definition list.
		all	Deletes all entries from the v3 user definition list.

Example

```
admin(system.snmp.access)>list acl
-----------------------------------------------------------------------------
index   start ip          end ip
-----------------------------------------------------------------------------
1       209.236.24.1      209.236.24.46

admin(system.snmp.access)>delete acl all
admin(system.snmp.access)>list acl
-----------------------------------------------------------------------------
index   start ip          end ip
-----------------------------------------------------------------------------
```

For information on configuring SNMP access settings using the applet (GUI), see "Configuring SNMP Access Control" on page 101.

AP4700>admin(system.snmp.access)>list

Lists SNMP access entries.

Syntax

list	acl		Lists SNMP access control list entries.
	v1v2c		Lists SNMP v1/v2c configuration.
	v3	<idx>	Lists SNMP v3 user definition by index <idx> (1-10).
		all	Lists all SNMP v3 user definitions.

Example

```
admin(system.snmp.access)>list acl
----------------------------------------------------------------
index  start ip         end ip
----------------------------------------------------------------
1      209.236.24.1     209.236.24.46

admin(system.snmp.access)>list v1v2c
----------------------------------------------------------------
index  community          access         oid
----------------------------------------------------------------
1      public             read only      1.3.6.1
2      private            read/write     1.3.6.1

admin(system.snmp.access)>list v3 2

index                             : 2
username                          : judy
access permission                 : read/write
object identifier                 : 1.3.6.1
security level                    : auth/priv
auth algorithm                    : md5
auth password                     : ********
privacy algorithm                 : des
privacy password                  : *******
```

For information on configuring SNMP access settings using the applet (GUI), see “Configuring SNMP Access Control” on page 101.

System SNMP Traps Commands

AP4700>admin(system.snmp.traps)

Displays the SNMP traps submenu. The items available under this command are shown below.

show	Shows SNMP trap parameters.
set	Sets SNMP trap parameters.
add	Adds SNMP trap entries.
delete	Deletes SNMP trap entries.
list	Lists SNMP trap entries.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP4700>admin(system.snmp.traps)>show

Shows SNMP trap parameters.

Syntax

show	trap	Shows SNMP trap parameter settings.
	rate-trap	Shows SNMP rate-trap parameter settings.

Example

```
admin(system.snmp.traps)>show trap

SNMP MU Traps
     mu associated                     : enable
     mu unassociated                   : disable
     mu denied association             : disable
     mu denied authentication          : disable

SNMP Traps
     snmp authentication failure       : disable
     snmp acl violation                : disable

SNMP Network Traps
     physical port status change       : enable
     denial of service                 : enable
     denial of service trap rate limit : 10 seconds

SNMP System Traps
     system cold start                 : disable
     system config changed             : disable
     rogue ap detection                : disable
     ap radar detection                : disable
     wpa counter measure               : disable
     mu hotspot status                 : disable
     vlan                              : disable
     lan monitor                       : disable
     DynDNS Update                     : enable
     wlan kerb auth failed             : disable
     wwan event                        : disable
```

For information on configuring SNMP traps using the applet (GUI), see “Enabling SNMP Traps” on page 103.

AP4700>admin(system.snmp.traps)>set

Sets SNMP trap parameters.

Syntax

set	mu-assoc	enable/disable			Enables/disables the MU associated trap.
	mu-unassoc	enable/disable			Enables/disables the MU unassociated trap.
	mu-deny-assoc	enable/disable			Enables/disables the MU association denied trap.
	mu-deny-auth	enable/disable			Enables/disables the MU authentication denied trap.
	snmp-auth	enable/disable			Enables/disables the authentication failure trap.
	snmp-acl	enable/disable			Enables/disables the SNMP ACL violation trap.
	port	enable/disable			Enables/disables the physical port status trap.
	dos-attack	enable/disable			Enables/disables the denial of service trap.
	interval	<rate>			Sets denial of service trap interval.
	cold	enable/disable			Enables/disables the system cold start trap.
	cfg	enable/disable			Enables/disables a configuration changes trap.
	rogue-ap	enable/disable			Enables/disables a trap when a rogue-ap is detected.
	ap-radar	enable/disable			Enables/disables the AP Radar Detection trap.
	wpa-counter	enable/disable			Enables/disables the WPA counter measure trap.
	hotspot-mu-status	enable/disable			Enables/disables the hotspot mu status trap.
	vlan	enable/disable			Enables/disables VLAN traps.
	lan-monitor	enable/disable			Enables/disables LAN monitor traps.
	rate	<rate>	<scope>	<value>	Sets the particular <rate> to monitor to <value> given the indicated <scope>. See table below for information on the possible values for <rate>, <scope>, and <value>.
	min-pkt	<pkt>			Sets the minimum number of packets required for rate traps to fire (1-65535).
	dyndns-update	enable/disable			Enables/disables dyndns update trap.
	wlan-kerb-auth-fail	enable/disable			Enables/disables the WLAN Kerberos authentication trap.
	wwan-event	enable/disable			Enables/disables the WWAN event trap.
	all	enable/disable			Enables/disables each trap.

For information on configuring SNMP traps using the applet (GUI), see "Configuring Specific SNMP Traps" on page 105.

AP4700>admin(system.snmp.traps)>add

Adds SNMP trap entries.

Syntax

add v1v2 <ip> <port> <comm> <ver>

Adds an entry to the SNMP v1/v2 access list with the destination IP address set to <ip>, the destination UDP port set to <port>, the community string set to <comm> (1 to 31 characters), and the SNMP version set to <ver>.

v3 <ip> <port> <user> <sec> <auth> <pass1> <priv> <pass2>

Adds an entry to the SNMP v3 access list with the destination IP address set to <ip>, the destination UDP port set to <port>, the username set to <user> (1 to 31 characters), and the authentication type set to one of none, auth, or auth/priv.

The following parameters must be specified if <sec> is not none:
Authentication type <auth> set to md5 or sha1
Authentication password <pass1> (8 to 31 chars)

The following parameters must be specified if <sec> is set to auth/priv:
Privacy algorithm set to des or aes
Privacy password <pass2> (8 to 31 chars)

Example

```
admin(system.snmp.traps)>add v1v2 203.223.24.2 333 mycomm v1
admin(system.snmp.traps)>list v1v2c
---------------------------------------------------------------------
index   dest ip          dest port      community        version
---------------------------------------------------------------------
1       203.223.24.2     333            mycomm           v1

admin(system.snmp.traps)>add v3 201.232.24.33 555 BigBoss none md5
admin(system.snmp.traps)>list v3 all

index                               : 1
destination ip                      : 201.232.24.33
destination port                    : 555
username                            : BigBoss
security level                      : none
auth algorithm                      : md5
auth password                       : ********
privacy algorithm                   : des
privacy password                    : ********
```

For information on configuring SNMP traps using the applet (GUI), see “Configuring SNMP RF Trap Thresholds” on page 107.

AP4700>admin(system.snmp.traps)>delete

Deletes SNMP trap entries.

Syntax

delete	v1v2c	<idx>	Deletes entry <idx> from the v1v2c access control list.
		all	Deletes all entries from the v1v2c access control list.
	v3	<idx>	Deletes entry <idx> from the v3 access control list.
		all	Deletes all entries from the v3 access control list.

Example

```
admin(system.snmp.traps)>delete v1v2 all
```

For information on configuring SNMP traps using the applet (GUI), see "Configuring SNMP Settings" on page 97.

AP4700>admin(system.snmp.traps)>list

Lists SNMP trap entries.

Syntax

list	v1v2c		Lists SNMP v1/v2c access entries.
	v3	<idx>	Lists SNMP v3 access entry <idx 1-10> .
		all	Lists all SNMP v3 access entries.

Example

```
admin(system.snmp.traps)>add v1v2 203.223.24.2 162 mycomm v1
admin(system.snmp.traps)>list v1v2c
----------------------------------------------------------------------
index   dest ip          dest port      community        version
----------------------------------------------------------------------
1       203.223.24.2     162            mycomm           v1

admin(system.snmp.traps)>add v3 201.232.24.33 555 BigBoss none md5
admin(system.snmp.traps)>list v3 all

index                              : 1
destination ip                     : 201.232.24.33
destination port                   : 555
username                           : BigBoss
security level                     : none
auth algorithm                     : md5
auth password                      : ********
privacy algorithm                  : des
privacy password                   : ********
```

For information on configuring SNMP traps using the applet (GUI), see “Configuring SNMP RF Trap Thresholds” on page 107.

System User Database Commands

AP4700>admin(system)> userdb

Goes to the user database submenu.

Syntax

user	Goes to the user submenu.
group	Goes to the group submenu.
save	Saves the configuration to system flash.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring User Database permissions using the applet (GUI), see "Defining User Access Permissions by Group" on page 259.

Adding and Removing Users from the User Databse

AP4700>admin(system.userdb)>user

Adds and removes users from the user database and defines user passwords.

Syntax

add	Adds a new user.
delete	Deletes a new user.
clearall	Removes all existing user IDs from the system.
set	Sets a password for a user.
show	Displays the current user database configuration.
save	Saves the configuration to system flash.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring User Database permissions using the applet (GUI), see "Defining User Access Permissions by Group" on page 259.

AP4700>admin(system.userdb.user)>add

Adds a new user to the user database.

Syntax

add	Adds a new user ID <userid> and password <passwd> string to the user database.

Example

```
admin(system.userdb.user>add george password

admin(system.userdb.user>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining User Access Permissions by Group" on page 259.

AP4700>admin(system.userdb.user)>delete

Removes a new user to the user database.

Syntax

delete	Removes a user ID <id> and password <pw> string from the user database.

Example

```
admin(system.userdb.user>delete george

admin(system.userdb.user>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining User Access Permissions by Group" on page 259.

AP4700>admin(system.userdb.user)>clearall

Removes all existing user IDs from the system.

Syntax

clearall	Removes all existing user IDs from the system.

Example

```
admin(system.userdb.user>clearall

admin(system.userdb.user>
```

For information on configuring User Database permissions using the applet (GUI), see “Defining User Access Permissions by Group” on page 259.

AP4700>admin(system.userdb.user)>set

Sets a password for a user.

Syntax

set	<userid> <passwd>	Sets user <userid> and password <passwd> string for a specific user.

Example

```
admin(system.userdb.user>set george password

admin(system.userdb.user>
```

For information on configuring User Database permissions using the applet (GUI), see “Defining User Access Permissions by Group” on page 259.

Adding and Removing Groups from the User Databse

AP4700>admin(system.userdb)>group

Adds and removes groups from the user database.

Syntax

create	Creates a group name.
delete	Deletes a group name.
clearall	Removes all existing group names from the system.
add	Adds a user to an existing group.
remove	Removes a user from an existing group.
show	Displays existing groups.
save	Saves the configuration to system flash.
..	Goes to the parent menu.
/	Moves back to root menu.

For information on configuring User Database permissions using the applet (GUI), see "Defining User Access Permissions by Group" on page 259.

AP4700>admin(system.userdb.group)>create

Creates a group name. Once defined, users can be added to the group.

Syntax

create	Creates a group name string. Once defined, users can be added to the group.

Example

```
admin(system.userdb.group>create 2

admin(system.userdb.group>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining User Access Permissions by Group" on page 259.

AP4700>admin(system.userdb.group)>delete

Deletes an existing group.

Syntax

delete	Deletes an existing group name string.

Example

```
admin(system.userdb.group>delete 2

admin(system.userdb.group>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining User Access Permissions by Group" on page 259.

AP4700>admin(system.userdb.group)>clearall

Removes all existing group names from the system.

Syntax

clearall	Removes all existing group names from the system.

Example

```
admin(system.userdb.group>clearall

admin(system.userdb.group>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining User Access Permissions by Group" on page 259.

AP4700>admin(system.userdb.group)>add

Adds a user to an existing group.

Syntax

add	<userid> <group>	Adds a user <userid> to an existing group <group>.

Example

```
admin(system.userdb.group>add lucy group x

admin(system.userdb.group>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining User Access Permissions by Group" on page 259.

AP4700>admin(system.userdb.group)>remove

Removes a user from an existing group.

Syntax

remove	<userid> <group>	Removes a user <userid> from an existing group<group>.

Example

```
admin(system.userdb.group>remove lucy group x

admin(system.userdb.group>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining User Access Permissions by Group" on page 259

AP4700>admin(system.userdb.group)>show

Displays existing groups.

Syntax

show		Displays existing groups and users,
	users	Displays configured user IDs for a group.
	groups	Displays configured groups.

Example

```
admin(system.userdb.group>show groups

List of Group Names
                       : engineering
                       : marketing
                       : demo room

admin(system.userdb.group>
```

For information on configuring User Database permissions using the applet (GUI), see “Defining User Access Permissions by Group” on page 259.

System RADIUS Commands

AP4700>admin(system)>radius

Goes to the RADIUS system submenu.

Syntax

eap	Goes to the EAP submenu.
policy	Goes to the access policy submenu.
ldap	Goes to the LDAP submenu.
proxy	Goes to the proxy submenu.
client	Goes to the client submenu.
set	Sets RADIUS parameters.
show	Displays RADIUS parameters.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring RADIUS using the applet (GUI), see "Configuring User Authentication" on page 250.

AP4700>admin(system.radius)>set/show

Sets or displays the RADIUS user database.

Syntax

set	Sets the RADIUS user database.
show all	Displays the RADIUS user database.

Example

```
admin(system.radius)>set database local
admin(system.radius)>show all

Database                : local

admin(system.radius)>
```

For information on configuring RADIUS using the applet (GUI), see "Configuring User Authentication" on page 250.

AP4700>admin(system.radius)>eap

Goes to the EAP submenu.

Syntax

peap	Goes to the Peap submenu.
ttls	Goes to the TTLS submenu.
import	Imports the requested EAP certificates.
set	Defines EAP parameters.
show	Displays the EAP configuration.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring EAP RADIUS using the applet (GUI), see “Configuring User Authentication” on page 250.

AP4700>admin(system.radius.eap)>peap

Goes to the Peap submenu.

Syntax

set	Defines Peap parameters.
show	Displays the Peap configuration.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring PEAP RADIUS using the applet (GUI), see “Configuring User Authentication” on page 250.

AP4700>admin(system.radius.eap.peap)>set/show

Defines and displays Peap parameters

Syntax

set	Sets the Peap authentication <peap type> (to either gtc or mschapv2).
show	Displays the Peap authentication type.

Example

```
admin(system.radius.eap.peap)>set auth gtc
admin(system.radius.eap.peap)>show

PEAP Auth Type                        : gtc
```

For information on configuring EAP PEAP RADIUS values using the applet (GUI), see “Configuring User Authentication” on page 250.

AP4700>admin(system.radius.eap)>ttls

Goes to the TTLS submenu.

Syntax

set	Defines TTLS parameters.
show	Displays the TTLS configuration.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring EAP TTLS RADIUS values using the applet (GUI), see "Configuring User Authentication" on page 250.

AP4700>admin(system.radius.eap.ttls)>set/show

Defines and displays TTLS parameters

Syntax

set	Sets the default TTLS authentication <ttls type> (to either pap, md5 or mschapv2).
show	Displays the TTLS authentication <type>.

Example

```
admin(system.radius.eap.ttls)>set auth pap
admin(system.radius.eap.ttls)>show

TTLS Auth Type                        : pap
```

For information on configuring EAP TTLS RADIUS values using the applet (GUI), see "Configuring User Authentication" on page 250.

AP4700>admin(system.radius)>policy

Goes to the access policy submenu.

Syntax

set	Sets a group’s WLAN access policy.
access-time	Goes to the time based login submenu.
show	Displays the group’s access policy.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring RADIUS access policies using the applet (GUI), see “Configuring User Authentication” on page 250.

AP4700>admin(system.radius.policy)>set

Defines the group's WLAN access policy.

Syntax

set	<group> <wlan(s) >	Defines a group's <group> WLAN access policy (defined as a string) delimited by a space.

Example

```
admin(system.radius.policy)>set engineering 16

admin(system.radius.policy)>
```

For information on configuring RADIUS WLAN policy values using the applet (GUI), see "Configuring User Authentication" on page 250.

AP4700>admin(system.radius.policy)>access-time

Goes to the time-based login submenu.

Syntax

set	<group> <access-time>	Defines a target group's access time permissions. Access time is in DayDDDD-DDDD format.
show		Displays the group's access time rule.
save		Saves the configuration to system flash.
quit		Quits the CLI.
..		Goes to the parent menu.
/		Goes to the root menu.

Example

```
admin(system.radius.policy.access-time)>show

List of Access Policies

1                      : Tue0830-2200, We2000-2300, Th1100-1930
2                      : Any0000-2359
10                     : Any0000-2359
12                     : Any0000-2359
```

Context	Command	Description

system>radius>policy>access-time	set start-time <group> <value>	group = Valid group name.
		value = 4 digit value representing HHMM
		(0000-2359 allowed).

system>radius>policy>access-time	set end-time <group> <value>	group = Valid group name.
		value = 4 digit value representing HHMM
		(0000-2359 allowed).
		The end time should be greater than the start time.

system>radius>policy>access-time	set access-days <group> <day-selector-keyword>	group = Valid group name. day-selector-keyword = The allowed values are: Mo, Tu, We, Th, Fr, Sa, Su, Weekdays, Weekends, all.

For information on configuring RADIUS WLAN policy values using the applet (GUI), see "Configuring User Authentication" on page 250.

AP4700>admin(system.radius.policy)>show

Displays a group’s access policy.

Syntax

show	Displays a group’s access policy.

Example

```
admin(system.radius.policy)>show

List of Access Policies

engineering                          : 16
marketing                            : 10
demo room                            : 3
test demo                            : No Wlans

admin(system.radius.policy)>
```

For information on configuring RADIUS WLAN policy values using the applet (GUI), see “Configuring User Authentication” on page 250

AP4700>admin(system.radius)>ldap

Goes to the LDAP submenu.

Syntax

set	Defines the LDAP parameters.
show all	Displays existing LDAP parameters.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring a RADIUS LDAP server using the applet (GUI), see "Configuring LDAP Authentication" on page 253.

AP4700>admin(system.radius.ldap)>set

Defines the LDAP parameters.

Syntax

set		Defines the LDAP parameters.
	ipadr	Sets LDAP IP address.
	port	Sets LDAP server port.
	binddn	Sets LDAP bind distinguished name.
	basedn	Sets LDAP base distinguished name.
	passwd	Sets LDAP server password.
	login	Sets LDAP login attribute.
	pass_attr	Sets LDAP password attribute.
	groupname	Sets LDAP group name attribute.
	filter	Sets LDAP group membership filter.
	membership	Sets LDAP group membership attribute.

Example

```
admin(system.radius.ldap)>set ipadr 157.235.121.12
admin(system.radius.ldap)>set port 1812
admin(system.radius.ldap)>set binddn 123
admin(system.radius.ldap)>set basedn 123
admin(system.radius.ldap)>set passwd mudskipper
admin(system.radius.ldap)>set login muddy
admin(system.radius.ldap)>set pass_attr 123
admin(system.radius.ldap)>set groupname 0.0.0.0
admin(system.radius.ldap)>set filter 123
admin(system.radius.ldap)>set membership radiusGroupName

admin(system.radius.ldap)>
```

For information on configuring a RADIUS LDAP server using the applet (GUI), see "Configuring LDAP Authentication" on page 253.

AP4700>admin(system.radius.ldap)>show all

Displays existing LDAP parameters.

Syntax

show all	Displays existing LDAP parameters.

Example

```
admin(system.radius.ldap)>show all

LDAP Server IP                    : 0.0.0.0
LDAP Server Port                  : 389
LDAP Bind DN                      : cn=manager, o=trion
LDAP Base DN                      : 0=trion
LDAP Login Attribute              : (uid=%{Stripped-User-Name:-%{User-Name}})
LDAP Password attribute           : userPassword
LDAP Group Name Attribue          : cn
LDAP Group Membership Filter      : (|(&(objectClass=GroupOfNames)(member=%{Ldap-
objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-UserDn})))
LDAP Group Membership Attribute   : radiusGroupName

admin(system.radius.ldap)>
```

For information on configuring a RADIUS LDAP server using the applet (GUI), see “Configuring LDAP Authentication” on page 253.

AP4700>admin(system.radius)>proxy

Goes to the RADIUS proxy server submenu.

Syntax

add	Adds a proxy realm.
delete	Deletes a proxy realm.
clearall	Removes all proxy server records.
set	Sets proxy server parameters.
show	Displays current RADIUS proxy server parameters.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring RADIUS proxy server values using the applet (GUI), see “Configuring a Proxy Radius Server” on page 255.

AP4700>admin(system.radius.proxy)>add

Adds a proxy.

Syntax

add			Adds a proxy realm.
	name	<name>	Realm name.
	ip1	<ip1>	Authentication server IP address.
	port	<port>	Authentication server port.
	sec	<sec>	Shared secret password.

Example

```
admin(system.radius.proxy)>add lancelot 157.235.241.22 1812 muddy

admin(system.radius.proxy)>
```

For information on configuring RADIUS proxy server values using the applet (GUI), see "Configuring a Proxy Radius Server" on page 255.

AP4700>admin(system.radius.proxy)>delete

Adds a proxy.

Syntax

delete	<realm>	Deletes a realm name.

Example

```
admin(system.radius.proxy)>delete lancelot

admin(system.radius.proxy)>
```

For information on configuring RADIUS proxy server values using the applet (GUI), see "Configuring a Proxy Radius Server" on page 255.

AP4700>admin(system.radius.proxy)>clearall

Removes all proxy server records from the system.

Syntax

clearall	Removes all proxy server records from the system.

Example

```
admin(system.radius.proxy)>clearall

admin(system.radius.proxy)>
```

For information on configuring RADIUS proxy server values using the applet (GUI), see "Configuring a Proxy Radius Server" on page 255.

AP4700>admin(system.radius.proxy)>set

Sets Radius proxy server parameters.

Syntax

set		Sets RADIUS proxy server parameters.
	delay	Defines retry delay time (in seconds) for the proxy server.
	count	Defines retry count value for the proxy server.

Example

```
admin(system.radius.proxy)>set delay 10
admin(system.radius.proxy)>set count 5

admin(system.radius.proxy)>
```

For information on configuring RADIUS proxy server values using the applet (GUI), see "Configuring a Proxy Radius Server" on page 255.

AP4700>admin(system.radius)>client

Goes to the RADIUS client submenu.

Syntax

add	Adds a RADIUS client to list of available clients.
delete	Deletes a RADIUS client from list of available clients.
show	Displays a list of configured clients.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring RADIUS client values using the applet (GUI), see "Configuring the Radius Server" on page 250.

AP4700>admin(system.radius.client)>add

Adds a RADIUS client to those available to the RADIUS server.

Syntax

add			Adds a proxy.
	ip	<ip>	Client’s IP address.
	mask	<ip1>	Network mask address of the client.
	secret	<sec>	Shared secret password.

Example

```
admin(system.radius.client)>add 157.235.132.11 255.255.255.225 muddy

admin(system.radius.client)>
```

For information on configuring RADIUS client values using the applet (GUI), see “Configuring the Radius Server” on page 250.

AP4700>admin(system.radius.client)>delete

Removes a specified RADIUS client from those available to the RADIUS server.

Syntax

delete	Removes a specified RADIUS client <ipadr> from those available to the RADIUS server.

Example

```
admin(system.radius.client)>delete 157.235.132.11

admin(system.radius.client)>
```

For information on configuring RADIUS client values using the applet (GUI), see "Configuring the Radius Server" on page 250.

AP4700>admin(system.radius.client)>show

Displays a list of configured RADIUS clients.

Syntax

show	Removes a specified RADIUS client from those available to the RADIUS server.

Example

```
admin(system.radius.client)>show
-----------------------------------------------------------------------------
Idx    Subnet/Host      Netmask            SharedSecret
-----------------------------------------------------------------------------
1      157.235.132.11   255.255.255.225    *****

admin(system.radius.client)>
```

For information on configuring RADIUS client values using the applet (GUI), see “Configuring the Radius Server” on page 250.

System Network Time Protocol (NTP) Commands

AP4700>admin(system)>ntp

Displays the NTP menu. The correct network time is required for numerous functions to be configured accurately on the access point.

Syntax

show	Shows NTP parameters settings.
date-zone	Show date, time and time zone.
zone-list	Displays list of time zones.
set	Sets NTP parameters.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

For information on configuring NTP using the applet (GUI), see "Configuring Network Time Protocol (NTP)" on page 110.

AP4700>admin(system.ntp)>show

Displays the NTP server configuration.

Syntax

show	Shows all NTP server settings.

Example

```
admin(system.ntp)>show

current time                      : 2006-07-31 14:35:20

time zone:                        : UTC

ntp mode                          : enable
```

For information on configuring NTP using the applet (GUI), see "Configuring Network Time Protocol (NTP)" on page 110.

AP4700>admin(system.ntp)>date-zone

Show date, time and time zone.

Syntax

date-zone	Show date, time and time zone.

Example

```
admin(system.ntp)>date-zone

Date/Time           : Sat 1970-Jan-03 20:06:22 +0000 UTC

Time Zone           : UTC
```

For information on configuring NTP using the applet (GUI), see “Configuring Network Time Protocol (NTP)” on page 110.

AP4700>admin(system.ntp)>zone-list

Displays an extensive list of time zones for countries around the world.

Syntax

zone-list	Displays list of time zone indexes for every known zone.

Example

```
admin(system.ntp)> zone-list
```

For information on configuring NTP using the applet (GUI), see “Configuring Network Time Protocol (NTP)” on page 110.

AP4700>admin(system.ntp)>set

Sets NTP parameters for access point clock synchronization.

Syntax

set	mode	<ntp-mode>	Enables or disables NTP.
	server	<idx> <ip>	Sets the NTP sever IP address.
	port	<idx> <port>	Defines the port number.
	intrvl	<period>	Defines the clock synchronization interval used between the access point and the NTP server in minutes (15 - 65535).
	time	<time>	Sets the current system time. [yyyy] - year, [mm] - month, [dd] - day of the month, [hh] - hour of the day, [mm] - minute, [ss] second, [zone -idx] Index of the zone.
	zone	<zone>	Defines the time zone (by index) for the target country.

Example

```
admin(system.ntp)>set mode enable
admin(system.ntp)>set server 1 203.21.37.18
admin(system.ntp)>set port 1 123
admin(system.ntp)>set intrvl 15
admin(system.ntp)>set zone 1
```

For information on configuring NTP using the applet (GUI), see "Configuring Network Time Protocol (NTP)" on page 110.

System Log Commands

AP4700>admin(system)>logs

Displays the access point log submenu. Logging options include:

Syntax

show	Shows logging options.
set	Sets log options and parameters.
view	Views system log.
delete	Deletes the system log.
send	Sends log to the designated FTP Server.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves configuration to system flash.
quit	Quits the CLI.

AP4700>admin(system.logs)>show

Displays the current access point logging settings.

Syntax

show	Displays the current access point logging configuration.

Example

```
admin(system.logs)>show

log level                          : L6 Info
syslog server logging              : enable
syslog server ip address           : 192.168.0.102
```

For information on configuring logging settings using the applet (GUI), see "Logging Configuration" on page 112.

AP4700>admin(system.logs)>set

Sets log options and parameters.

Syntax

set	level	<level>	Sets the level of the events that will be logged. All events with a level at or above <level> (L0-L7) will be saved to the system log. L0:Emergency L1:Alert L2:Critical L3:Errors L4:Warning L5:Notice L6:Info *(default setting)* L7:Debug
	mode	<mode>	Enables or disables syslog server logging.
	ipadr	<ip>	Sets the external syslog server IP address to <ip> (a.b.c.d).

```
admin(system.logs)>set mode enable
admin(system.logs)>set level L4
admin(system.logs)>set ipadr 157.235.112.11
```

For information on configuring logging settings using the applet (GUI), see "Logging Configuration" on page 112.

AP4700>admin(system.logs)>view

Displays the access point system log file.

Syntax

view	Displays the entire access point system log file.

Example

```
admin(system.logs)>view

Jan  7 16:14:00 (none) syslogd 1.4.1: restart (remote reception).
Jan  7 16:14:10 (none) klogd: :ps log:fc: queue maintenance
Jan  7 16:14:41 (none) klogd: :ps log:fc: queue maintenance
Jan  7 16:15:43 (none) last message repeated 2 times
Jan  7 16:16:01 (none) CC:   4:16pm  up 6 days, 16:16, load average: 0.00, 0.01,
 0.00
Jan  7 16:16:01 (none) CC:   Mem:        62384        32520        29864
    0            0
Jan  7 16:16:01 (none) CC: 0000077e  0012e95b 0000d843 00000000 00000003 0000121
e 00000000 00000000  0037ebf7 000034dc 00000000 00000000 00000000
Jan  7 16:16:13 (none) klogd: :ps log:fc: queue maintenance
Jan  7 16:16:44 (none) klogd: :ps log:fc: queue maintenance
Jan  7 16:17:15 (none) klogd: :ps log:fc: queue maintenance
Jan  7 16:17:15 (none) klogd: :ps log:fc: queue maintenance
```

For information on configuring logging settings using the applet (GUI), see “Logging Configuration” on page 112.

AP4700>admin(system.logs)>delete

Deletes the log files.

Syntax

delete	Deletes the access point system log file.

Example

```
admin(system.logs)>delete
```

For information on configuring logging settings using the applet (GUI), see "Logging Configuration" on page 112.

AP4700>admin(system.logs)>send

Sends log and core file to an FTP Server.

Syntax

send	Sends the system log file via FTP to a location specified with the set command. Refer to the command set under the AP4700>admin(fw update) command for information on setting up an FTP server and login information.

Example

```
admin(system.logs)>send

File transfer                          : [ In progress ]
File transfer                          : [ Done ]

admin(system.logs)>
```

For information on configuring logging settings using the applet (GUI), see “Logging Configuration” on page 112.

System Configuration-Update Commands

AP4700>admin(system.config)>

Displays the access point configuration update submenu.

Syntax

default	Restores the default access point configuration.
partial	Restores a partial default access point configuration.
show	Shows import/export parameters.
set	Sets import/export access point configuration parameters.
export	Exports access point configuration to a designated system.
import	Imports configuration to the access point.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to access point system flash.
quit	Quits the CLI.

AP4700>admin(system.config)>default

Restores the full access point factory default configuration.

Syntax

default	Restores the access point to the original (factory) configuration.

Example

```
admin(system.config)>default

Are you sure you want to default the configuration? <yes/no>:
```

For information on importing/exporting access point configurations using the applet (GUI), see "Importing/Exporting Configurations" on page 114.

AP4700>admin(system.config)>partial

Restores a partial factory default configuration. The access point's LAN, WAN and SNMP settings are unaffected by the partial restore.

Syntax

default	Restores a partial access point configuration.

Example

```
admin(system.config)>partial

Are you sure you want to partially default AP4700? <yes/no>:
```

For information on importing/exporting access point configurations using the applet (GUI), see "Importing/Exporting Configurations" on page 114.

AP4700>admin(system.config)>show

Displays import/export parameters for the access point configuration file.

Syntax

show	Shows all import/export parameters.

Example

```
admin(system.config)>show

cfg filename                       : cfg.txt
cfg filepath                       :
ftp/tftp server ip address         : 192.168.0.101
ftp user name                      : myadmin
ftp password                       : ********
```

For information on importing/exporting access point configurations using the applet (GUI), see "Importing/Exporting Configurations" on page 114.

AP4700>admin(system.config)>set

Sets the import/export parameters.

Syntax

set	file	<filename>	Sets the configuration file name (1 to 39 characters in length).
	path	<path>	Defines the path used for the configuration file upload.
	server	<ipaddress>	Sets the FTP/TFTP server IP address.
	user	<username>	Sets the FTP user name (1 to 39 characters in length).
	passwd	<pswd>	Sets the FTP password (1 to 39 characters in length).

Example

```
admin(system.config)>set server 192.168.22.12
admin(system.config)>set user myadmin
admin(system.config>set passwd georges

admin(system.config)>show

cfg filename                       : cfg.txt
cfg filepath                       :
ftp/tftp server ip address         : 192.168.22.12
ftp user name                      : myadmin
ftp password                       : *******
```

For configuration file creation and export, only the set radio-config is supported. Therefore, when configuration files for export are created, a line such as `set rf-function X wips / wlan` (where X is 1 or 2) is never be generated.

For configuration file import, the legacy command `set rf-function X wips / wlan` is processed as it has historically.

There is no CLI menu allowing the user to enter `set rf-function X wips/wlan` (where X is 1 or 2).

Instead, the command `set radio-configX` (where X is 1,2,3,4,5,6,7, or 8) is created in the configuration files for export.

For information on importing/exporting access point configurations using the applet (GUI), see "Importing/Exporting Configurations" on page 114.

AP4700>admin(system.config)>export

Exports the configuration from the system.

Syntax

export	ftp	Exports the access point configuration to the FTP server. Use the set command to set the server, user, password, and file name before using this command.
	tftp	Exports the access point configuration to the TFTP server. Use the set command to set the IP address for the TFTP server before using the command.
	terminal	Exports the access point configuration to a terminal.
	sftp	Exports the access point configuration to the SFTP server. Use the set command to set the server, user, password, and file name before using this command.

Example

Export FTP or SFTP Example

```
admin(system.config)>set server 192.168.22.12
admin(system.config)>set user myadmin
admin(system.config)>set file config.txt
admin(system.config)>set passwd

admin(system.config)>export ftp/export sftp

Export operation                 : [ Started ]
Building configuration file      : [ Done ]
File transfer                    : [ In progress ]
File transfer                    : [ Done ]
Export Operation                 : [ Done ]
```

Export TFTP Example

```
admin(system.config)>set server 192.168.0.101
admin(system.config)>set file config.txt
admin(system.config)>export tftp

Export operation                  : [ Started ]
Building configuration file       : [ Done ]
File transfer                     : [ In progress ]
File transfer                     : [ Done ]
Export Operation                  : [ Done ]
```

CAUTION

Make sure a copy of the access point’s current configuration is exported (to a secure location) before exporting the access point’s configuration, as you will want a valid version available in case errors are encountered with the configuration export.

For information on importing/exporting access point configurations using the applet (GUI), see “Importing/Exporting Configurations” on page 114.

AP4700>admin(system.config)>import

Imports the access point configuration to the access point. Errors could display as a result of invaid configuration parameters. Correct the sepcified lines and import the file again until the import operation is error free.

import	ftp	Imports the access point configuration file from the FTP server. Use the set command to set the server, user, password, and file.
	tftp	Imports the access point configuration from the TFTP server. Use the set command to set the server and file.
	sftp	Imports the access point configuration from the SFTP server. Use the set command to set the server and file.

Example

Import FTP Example

```
admin(system.config>set server 192.168.22.12
admin(system.config>set user myadmin
admin(system.config)>set file config.txt
admin(system.config)>set passwd mysecret
admin(system.config)>import ftp
Import operation : [ Started ]
File transfer : [ In progress ]
File transfer : [ Done ]
Import operation : [ Done ]
```

Import TFTP Example

```
admin(system.config)>set server 192.168.0.101
admin(system.config)>set file config.txt
admin(system.config)>import tftp
Import operation : [ Started ]
File transfer : [ In progress ]
File transfer : [ Done ]
Import operation : [ Done ]
```

CAUTION

A single-radio model access point cannot import/export its configuration to a dual-radio model access point. In turn, a dual-radio model access point cannot import/export its configuration to a single-radio access point.

CAUTION

Extreme Networks discourages importing a 1.0 baseline configuration file to a 1.1 (or later) version access point. Similarly, a 2.0 baseline configuration file should not be imported to a 1.0 version access point. Importing configurations between different version access point's results in broken configurations, since new features added to the 2.0 version access point cannot be supported in a leagcy version access point.

For information on importing/exporting access point configurations using the applet (GUI), see "Importing/Exporting Configurations" on page 114.

Firmware Update Commands

AP4700>admin(system)>fw-update

Displays the firmware update submenu. The items available under this command are shown below.

NOTE

The access point must complete the reboot process to successfully update the device firmware, regardless of whether the reboot is conducted uing the GUI or CLI interfaces.

show	Displays the current access point firmware update settings.
set	Defines the access point firmware update parameters.
update	Executes the firmware update.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the current configuration to the access point system flash.
quit	Quits the CLI and exits the current session.

AP4700>admin(system.fw-update)>show

Displays the current access point firmware update settings.

Syntax

show	Shows the current system firmware update settings for the access point.

Example

```
admin(system.fw-update)>show

automatic firmware upgrade                : enable
automatic config upgrade                  : enable

firmware filename                         : apn.bin
firmware path                             : /tftpboot/
ftp/tftp server ip address                : 168.197.2.2
ftp user name                             : jsmith
ftp password                              : *******
```

For information on updating access point device firmware using the applet (GUI), see "Updating Device Firmware" on page 118.

AP4700>admin(system.fw-update)>set

Defines access point firmware update settings and user permissions.

Syntax

set	fw-auto	<mode>	When enabled, updates device firmware each time the firmware versions are found to be different between the access point and the specified firmware on the remote system.
	cfg-auto	<mode>	When enabled, updates device configuration file each time the confif file versions are found to be different between the access point and the specified LAN or WAN interface.
	file	<name>	Defines the firmware file name (1 to 39 characters).
	path	<path>	Specifies a path for the file (1 to 39 characters).
	server	<ip>	The IP address for the FTP/TFTP server used for the firmware and/or config file update.
	user	<name>	Specifies a username for FTP server login (1 to 39 characters).
	passwd	<password>	Specifies a password for FTP server login (1 to 39 characters). Default is extreme.

```
admin(system.fw-update)>set fw-auto enable
admin(system.fw-update)>set cfg-auto enable
admin(system.fw-update)>set file 3.0.0.0-29D
admin(system.fw-update)>set path c:/fw
admin(system.fw-update)>set server 157.235.111.22
admin(system.fw-update)>set user mudskipper
admin(system.fw-update)>set passwd muddy
```

For information on updating access point device firmware using the applet (GUI), see "Updating Device Firmware" on page 118.

AP4700>admin(system.fw-update)>update

Executes the access point firmware update over the WAN or LAN ports using either ftp, tftp or SFTP.

Syntax

update	<mode><iface>	Defines the ftp ot tftp mode used to conduct the firmware update. Specifies whether the update is executed over the access point's WAN, LAN1 or LAN2 interface <iface>.

NOTE

The access point must complete the reboot process to successfully update the device firmware, regardless of whether the reboot is conducted uing the GUI or CLI interfaces.

```
admin(system.fw-update)>update ftp
```

For information on updating access point device firmware using the applet (GUI), see "Updating Device Firmware" on page 118.

Statistics Commands

AP4700>admin(stats)

Displays the access point statistics submenu. The items available under this command are:

show	Displays access point WLAN, MU, LAN and WAN statistics.
send-cfg-ap	Sends a config file to another access point within the known AP table.
send-cfg-all	Sends a config file to all access points within the known AP table.
clear	Clears all statistic counters to zero.
flash-all-leds	Starts and stops the flashing of all access point LEDs.
echo	Defines the parameters for pinging a designated station.
ping	Iniates a ping test.
..	Moves to the parent menu.
/	Goes to the root menu.
save	Saves the current configuration to system flash.
quit	Quits the CLI.

AP4700>admin(stats)>show

Displays access point system information.

Syntax

show	wan	Displays stats for the access point WAN port.
	lan	Displays stats for the access point LAN port
	stp	Displays LAN Spanning Tree Status
	wlan	Displays WLAN status and statistics summary.
	s-wlan	Displays status and statistics for an individual WLAN
	radio	Displays a radio statistics transmit and receive summary.
	s-radio	Displays radio statistics for a single radio
	retry-hgram	Displays a radio's retry histogram statistics.
	mu	Displays all mobile unit (MU) status.
	s-mu	Displays status and statistics for an individual MU.
	auth-mu	Displays single MU Authentication statistics.
	mesh	Displays Wireless Bridge Statistics statistics summary.
	s-mesh	Displays single Wirless Bridge statistics.
	known-ap	Displays a Known AP summary.
	packets_per_legacy_rate	Displays packets for legacy rates for a defined index.
	packets_per_mcs_rate	Displays packets for mcs rates for a defined index.

For information on displaying WAN port statistics using the applet (GUI), see "Viewing WAN Statistics" on page 263.

For information on displaying LAN port statistics using the applet (GUI), see "Viewing LAN Statistics" on page 266.

For information on displaying Wireless statistics using the applet (GUI), see "Viewing Wireless Statistics" on page 271.

For information on displaying Radio statistics using the applet (GUI), see "Viewing Radio Statistics Summary" on page 276.

For information on displaying MU statistics using the applet (GUI), see "Viewing MU Statistics Summary" on page 281.

For information on displaying Mesh statistics using the applet (GUI), see "Viewing the Mesh Statistics Summary" on page 286.

For information on displaying Known AP statistics using the applet (GUI), see "Viewing Known Access Point Statistics" on page 288.

AP4700>admin(stats)>send-cfg-ap

Copies the access point's configuration to another access point within the known AP table.

Syntax

send-cfg-ap	<index>	Copies the access point's configuration to the access points within the known AP table. Mesh configuration attributes do not get copied using this command and must be configured manually.

Example

```
admin(stats)>send-cfg-ap 2
admin(stats)>
```

NOTE

The send-cfg-ap command copies all existing configuration parameters except Mesh settings, LAN IP data, WAN IP data and DHCP Server parameter information.

For information on copying the access point config to another access point using the applet (GUI), see "Viewing Known Access Point Statistics" on page 288.

AP4700>admin(stats)>send-cfg-all

Copies the access point’s configuration to all of the access points within the known AP table.

Syntax

send-cfg-all	Copies the access point’s configuration to all of the access points within the known AP table.

Example

```
admin(stats)>send-cfg-all
admin(stats)>
```

NOTE

The send-cfg-all command copies all existing configuration parameters except Mesh settings, LAN IP data, WAN IP data and DHCP Server parameter information.

For information on copying the access point config to another access point using the applet (GUI), see “Viewing Known Access Point Statistics” on page 288.

AP4700>admin(stats)>clear

Clears the specified statistics counters to zero to begin new data calculations.

Syntax

clear	wan	Clears WAN statistics counters.
	lan	Clears LAN statistics counters for specified LAN index (either clear lan 1 or clear lan 2).
	all-rf	Clears all RF data.
	all-wlan	Clears all WLAN summary information.
	wlan	Clears individual WLAN statistic counters.
	all-radio	Clears access point radio summary information.
	radio1	Clears statistics counters specific to radio1.
	radio2	Clears statistics counters specific to radio2.
	all-mu	Clears all MU statistic counters.
	mu	Clears MU statistics counters.
	known-ap	Clears Known AP statistic counters.

AP4700>admin(stats)>flash-all-leds

Starts and stops the illumination of a specified access point's LEDs.

Syntax

flash-all-leds	<index>	Defines the Known AP index number of the target AP to flash.
	<stop/start>	Begins or terminates the flash activity.

Example

```
admin(stats)>

admin(stats)>flash-all-leds 1 start
Password ********
admin(stats)>flash-all-leds 1 stop
admin(stats)>
```

For information on flashing access point LEDs using the applet (GUI), see "Viewing Known Access Point Statistics" on page 288.

AP4700>admin(stats)>echo

Defines the echo test values used to conduct a ping test to an associated MU.

Syntax

show	Shows the Mobile Unit Statistics Summary.
list	Defines echo test parameters and result.
set	Determines echo test packet data.
start	Begins echoing the defined station.
..	Goes to parent menu.
/	Goes to root menu.
quit	Quits CLI session.

For information on MU Echo and Ping tests using the applet (GUI), see “Pinging Individual MUs” on page 285.

AP4700>admin.stats.echo)>show

Shows Mobile Unit Statistics Summary.

Syntax

show	Shows Mobile Unit Statistics Summary.

Example

```
admin(stats.echo)>show

-----------------------------------------------------------------------------
Idx    IP Address    MAC Address      WLAN    Radio    T-put    ABS    Retries
-----------------------------------------------------------------------------
1      192.168.2.0   00:A0F8:72:57:83 demo    11a
```

For information on MU Echo and Ping tests using the applet (GUI), see “Pinging Individual MUs” on page 285.

AP4700>admin.stats.echo)>list

Lists echo test parameters and results.

Syntax

list	Lists echo test parameters and results.

Example

```
admin(stats.echo)>list

Station Address              : 00A0F8213434
Number of Pings              : 10
Packet Length                : 10
Packet Data (in HEX)         : 55

admin(stats.echo)>
```

For information on MU Echo and Ping tests using the applet (GUI), see "Pinging Individual MUs" on page 285.

AP4700>admin.stats.echo)>set

Defines the parameters of the echo test.

Syntax

set	station	<mac>	Defines MU target MAC address.
	request	<num>	Sets number of echo packets to transmit (1-539).
	length	<num>	Determines echo packet length in bytes (1-539).
	data	<hex>	Defines the particular packet data.

For information on MU Echo and Ping tests using the applet (GUI), see "Pinging Individual MUs" on page 285.

AP4700>admin.stats.echo)>start

Initiates the echo test.

Syntax

start	Initiates the echo test.

Example

```
admin(stats.echo)>start

admin(stats.echo)>list

Station Address             : 00A0F843AABB
Number of Pings             : 10
Packet Length               : 100
Packet Data (in HEX)        : 1

Number of MU Responses      : 2
```

For information on MU Echo and Ping tests using the applet (GUI), see “Pinging Individual MUs” on page 285.

AP4700>admin(stats)>ping

Defines the ping test values used to conduct a ping test to an AP with the same ESSID.

Syntax

ping	show	Shows Known AP Summary details.
	list	Defines ping test packet length.
	set	Determines ping test packet data.
	start	Begins pinging the defined station.
	..	Goes to parent menu.
	/	Goes to root menu.
	quit	Quits CLI session.

For information on Known AP tests using the applet (GUI), see "Pinging Individual MUs" on page 285.

AP4700>admin.stats.ping)>show

Shows Known AP Summary Details.

Syntax

show	Shows Known AP Summary Details.

Example

```
admin(stats.ping)>show
-----------------------------------------------------------------------------
Idx     IP Address     MAC Address        MUs      KBIOS      Unit Name
-----------------------------------------------------------------------------
1       192.168.2.0    00:A0F8:72:57:83   3        0          Access Point
```

AP4700>admin.stats.ping)>list

Lists ping test parameters and results.

Syntax

list	Lists ping test parameters and results.

Example

```
admin(stats.ping)>list

Station Address             : 00A0F8213434
Number of Pings             : 10
Packet Length               : 10
Packet Data (in HEX)        : 55

admin(stats.ping)>
```

For information on Known AP tests using the applet (GUI), see "Pinging Individual MUs" on page 285.

AP4700>admin.stats.ping)>set

Defines the parameters of the ping test.

Syntax

set	station	Defines the AP target MAC address.
	request	Sets number of ping packets to transmit (1-539).
	length	Determines ping packet length in bytes (1-539).
	data	Defines the particular packet data.

Example

```
admin(stats.ping)>set station 00A0F843AABB
admin(stats.ping)>set request 10
admin(stats.ping)>set length 100
admin(stats.ping)>set data 1

admin(stats.ping)>
```

For information on Known AP tests using the applet (GUI), see "Pinging Individual MUs" on page 285.

AP4700>admin.stats.echo)>start

Initiates the ping test.

Syntax

start	Initiates the ping test.

Example

```
admin(stats.ping)>start

admin(stats.ping)>list

Station Address              : 00A0F843AABB
Number of Pings              : 10
Packet Length                : 100
Packet Data (in HEX)         : 1

Number of AP Responses       : 2
```

For information on Known AP tests using the applet (GUI), see “Pinging Individual MUs” on page 285.

9 CHAPTER Configuring Mesh Networking

Mesh provides a network that is robust and reliable. In this network, each node is connected to its neighbor by more than one path. The multiple paths provide the network with its robustness. If a node goes down, there are other paths available for the data to traverse through the network. Refer to the following for Mesh Network configuration activities supported by the access point user interface:

- Mesh Networking Overview on page 577
- Configuring Mesh Networking Support on page 581
- Mesh Network Deployment - Quick Setup on page 590
- Mesh Networking Frequently Asked Questions on page 601

Mesh Networking Overview

The Access Point can be configured in two modes to support the new mesh networking functionality. The Access Point can be set to a client bridge mode and/or a base bridge mode (which accepts connections from client bridges). Base bridge and client bridge mode can be used at the same time by an individual Access Point to optimally bridge traffic to other members of the mesh network and service associated MUs.

An Access Point in client bridge mode scans to locate other Access Points using the WLAP client's ESSID. Then it is required to go through the association and authentication process to establish wireless connections with the located devices. This association process is identical to the Access Point’s current MU association process. Once the association and authentication process is complete, the wireless client adds the connection as a port on its bridge module. This causes the client bridge to begin forwarding packets to the base bridge node. The base bridge realizes it is talking to a wireless client bridge. It then adds that connection as a port on its own bridge module. The two bridges at that point are communicating using the *Spanning Tree Protocol* (STP).

Access Points configured as both a base and a client bridge function as *repeaters* to transmit data with associated MUs in their coverage area (client bridge mode) as well as forward traffic to other Access Points in the mesh network (base bridge mode). The number of Access Points and their intended function within the mesh network dictate whether they should be configured as base bridges, client bridges or both (repeaters).

The spanning tree determines the path to the root and detects if the current connection is part of a network loop with another connection in the system. Each bridge can be configurable so the administrator can control the spanning tree to define the root bridge and what the forwarding paths are.

Once the spanning tree converges, both Access Points begin learning which destinations reside on which side of the network. This allows them to forward traffic intelligently.

After the client bridge establishes at least one wireless connection (if configured to support mobile users), it begins beaconing and accepting wireless connections. If configured as both a client bridge and a base bridge, it begins accepting client bridge connections. Therefore, the mesh network could connect simultaneously to different networks in a manner whereby a network loop is not created and then the connection is not blocked. Once the client bridge establishes at least one wireless connection, it begins establishing other wireless connections as it finds them available. Thus, the client bridge is able to establish simultaneous redundant links.

A mesh network must use one of the two Access Point LANs. If intending to use the Access Point for mesh networking support, Extreme Networks recommends configuring at least one WLAN (of the 16 WLANs available) specifically for mesh networking support.

The client bridge creates up to three connections if it can find base bridges for connection. If the connections are redundant (on the same network), then one connection will be forwarding and the others blocked. However, if each of the connections links to a different wired network, then none are redundant and all are forwarding. Thus, the bridge automatically detects and disables redundant connections, but leaves non-redundant connections forwarding. This gives the user the freedom to configure their topology in a variety of ways without limitations. This is important when configuring multiple Access Points for base bridge support in areas like a shipping yard where a large radio coverage area is required. For more information on configuring the Access Point in respect to specific usage scenarios, see "Mesh Network Deployment - Quick Setup" on page 590.

NOTE

Since each Access Point can establish up to 3 simultaneous wireless connections, some of these connections could be redundant. If this is the case, the STP algorithm defines which links are the redundant links and disables those links from forwarding.

If an Access Point is configured as a base bridge (but not as a client bridge) it operates normally at boot time. The base bridge supports connections made by other client bridges.

The dual-radio model Access Point affords users better optimization of the mesh networking feature by enabling the Access Point to transmit to other mesh network members using one independent radio and transmit with associated MUs using the second independent radio.

CAUTION

Only Extreme Networks AP4700 or AP3500 series model access points can be used as base bridges, client bridges or repeaters within an access point supported mesh network. If utilizing a mesh network, Extreme Networks recommends considering a dual-radio model to optimize channel utilization and throughput.

The Client Bridge Association Process

An Access Point in client bridge mode performs an active scan to quickly create a table of the Access Points nearby. The table contains the Access Points matching the ESS of the client bridge AP's WLAN. The table is used to determine the best Access Point to connect to (based on signal strength, load and the user's configured preferred connection list).

The association and authentication process is identical to the MU association process. The client Access Point sends 802.11 authentication and association frames to the base Access Point. The base Access Point responds as if the client is an actual mobile unit. Depending on the security policy, the two Access Point's engage in the normal handshake mechanism to establish keys.

After device association, the two Access Points are connected and the system can establish the bridge and run the spanning tree algorithm. In the meantime, the Access Point in client bridge mode continues to scan in the background attempts to establish an association with other Access Points using the same ESS on the same channel.

CAUTION

An Access Point is Base Bridge mode logs out whenever a Client Bridge associates to the Base Bridge over the LAN connection. This problem is not experienced over the Access Point's WAN connection. If this situation is experienced, log-in to the Access Point again.

The Access Point in client bridge mode attempts to establish up to 3 simultaneous wireless connections. The second and third connections are established in the background while the system is running. The first connection needs to be established before the system starts bridging traffic.

The dual-radio model Access Point affords users better optimization of the mesh networking feature by allowing the Access Point to transmit to other Access Points (in base or client bridge mode) using one independent radio and transmit with its associated MUs using the second independent radio.

Client Bridge Configuration Process Example

In this example, two Access Points are described with the following configurations:

- AP #1 base bridge
- AP #2 repeater (both a base and client bridge)

In the case of a mesh enabled radio, the client bridge configuration always takes precedence over the base bridge configuration. Therefore, when a radio is configured as a repeater (AP #2), the base bridge configuration takes effect only after the client bridge connection to AP #1 is established. Thus, AP #2 keeps scanning to find the base bridge, form the uplink and start beaconing as a base bridge for downstream client bridge connection. This is by design, as there is no reason to use a partially broken connection with no uplink to a base bridge.

Spanning Tree Protocol (STP)

The Access Point performs mesh networking using STP as defined in the 802.1d standard.

Once device association is complete, the client and base bridge exchange *Configuration Bridge Protocol Data Units* (BPDUs) to determine the path to the root. STP also determines whether a given port is a redundant connection or not.

Defining the Mesh Topology

When a user wants to control how the spanning tree determines client bridge connections, they need to control the mesh configuration. The user must be able to define one node as the root. Assigning a base bridge the lowest bridge priority defines it as the root.

NOTE

Extreme Networks recommends using the Mesh STP Configuration screen to define a base bridge as a root. Only advanced users should use the Advanced Client Bridge Settings screen's Preferred List to define the mesh topology, as omitting a bridge from the preferred list could break connections within the mesh network.

The Access Point can manipulate the path cost assigned to a bridge connection based on that connection's RSSI. This results in the spanning tree selecting the optimal path for forwarding data when redundant paths exist. However, this can be overridden using the preferred list. When using the preferred list, the user enters a priority for each bridge, resulting in the selection of the forwarding link.

Limit the wireless client's connections to reduce the number of hops required to get to the wired network. Use each radio's *preferred* base bridge list to define which Access Points the client bridge connects to. For more information, see "Configuring Mesh Networking Support" on page 581.

Mesh Networking and the Access Point's Two Subnets

The Access Point now has a second subnet on the LAN side of the system. This means wireless clients communicating through the same radio can reside on different subnets. The addition of this feature adds another layer of complexity to the Access Point's mesh networking functionality.

With a second LAN introduced, the LAN's Ethernet port (and any of the 16 WLANs) could be assigned to one of two different subnets. From a layer 2 perspective, the system has two different bridge functionalities, each with its own STP. The WLAN assignment controls the subnet (LAN1 or 2) upon which a given connection resides. If WLAN2 is assigned to LAN1, and WLAN2 is used to establish a client bridge connection, then the mesh network connection resides on LAN1.

Therefore, (depending upon the WLAN-to-LAN mapping), the Access Point could have multiple mesh connections on either LAN1 or LAN2.

Normal Operation

Once the mesh network is defined, all normal Access Point operations are still allowed. MUs are still allowed to associate with the Access Point as usual. The user can create WLANs, security polices and VLANs as with any other Access Point. DHCP services function normally and all layer 3 communications are allowed.

WNMP is used to send information about each mesh network so information can be displayed to the user from any Access Point on the system. WNMP messages are AP-AP info messages used to send system status.

Impact of Importing/Exporting Configurations to a Mesh Network

When using the Access Point's Configuration Import/Export screen to migrate an Access Point's configuration to other Access Points, mesh network configuration parameters will get sent or saved to other Access Points. However, if using the Known AP Statistics screen's Send Cfg to APs functionality, "auto-select" and preferred list" settings do not get imported.

CAUTION

When using the Import/Export screen to import a mesh supported configuration, do not import a base bridge configuration into an existing client bridge, as this could cause the mesh configuration to break.

Configuring Mesh Networking Support

Configuring the Access Point for Mesh Bridging support entails:

- Setting the LAN Configuration for Mesh Networking Support on page 581
- Configuring a WLAN for Mesh Networking Support on page 583
- Configuring the Access Point Radio for Mesh Support on page 585.

Setting the LAN Configuration for Mesh Networking Support

At least one of the two Access Point LANs needs to be enabled and have a mesh configuration defined to correctly function as a base or client bridge within a mesh network. This section describes the configuration activities required to define a mesh network's LAN configuration.

As the *Spanning Tree Protocol* (STP) mentions, each mesh network maintains hello, forward delay and max age timers. The base bridge defined as the root imposes these settings within the mesh network. The user does not necessarily have to change these settings, as the default settings will work. However, Extreme Networks encourages the user to define an Access Point as a base bridge and root (using the base bridge priority settings within the Bridge STP Configuration screen). Members of the mesh network can be configured as client bridges or additional base bridges with a higher priority value.

NOTE

For an overview on mesh networking and some of the implications on using the feature with the Access Point, see "Configuring Mesh Networking Support" on page 581.

To define a LAN's Mesh STP Configuration:

1 Select *Network Configuration* > *LAN* from the menu tree.

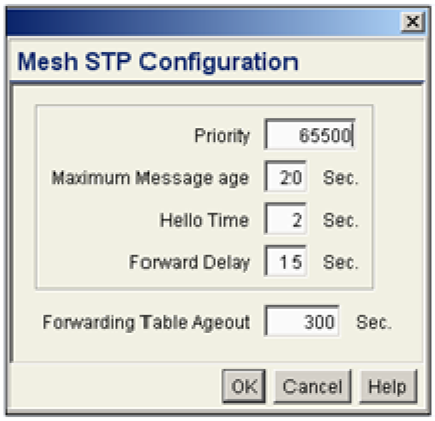
2 Enable the LAN used to support the mesh network.

   Verify the enabled LAN is named appropriately in respect to its intended function in supporting the mesh network.

3 Select *Network Configuration* > *LAN* > *LAN1 or LAN2* from the menu tree.

4 Click the *Mesh STP Configuration* button on the bottom off the screen.

5 Define the properties for the following parameters within the mesh network:



Mesh STP Configuration

Priority 65500

Maximum Message age 20 Sec.

Hello Time 2 Sec.

Forward Delay 15 Sec.

Forwarding Table Ageout 300 Sec.

Priority	Set the *Priority* as low as possible to force other devices within the mesh network to defer to this client bridge as the bridge defining the mesh configuration (commonly referred to as the root). Extreme Networks recommends assigning a Base Bridge AP with the lowest bridge priority so it becomes the root in the STP. If a root already exists, set the Bridge Priorities of new APs accordingly so the root of the STP doesn't get altered. Each Access Point starts with a default bridge priority of 63335.
Maximum Message age	The *Maximum Message age* timer is used with the Message Age timer. The Message Age timer is used to measure the age of the received protocol information recorded for a port, and to ensure the information is discarded when it exceeds the value set for the Maximum Message age timer.
Hello Time	The *Hello Time* is the time between each bridge protocol data unit sent. This time is equal to 2 seconds (sec) by default, but you can tune the time to be between 1 and 10 sec. If you drop the hello time from 2 sec to 1 sec, you double the number of bridge protocol data units sent/ received by each bridge. The 802.1d specification recommends the Hello Time be set to a value less than half of the Max Message age value.
Forward Delay	The *Forward Delay* is the time spent in the listening and learning state. This time is equal to 15 sec by default, but you can tune the time to be between 4 and 30 sec. The 802.1d specification recommends the Forward Delay be set to a value greater than half the Max Message age timeout value.
Forwarding Table Ageout	The Forwarding Table Parameter value defines the length of time an entry will remain in the a bridge's forwarding table before being deleted due to lack of activity. If the entry replenishments a destination generating continuous traffic, this timeout value will never be invoked. However, if the destination becomes idle, the timeout value represents the length of time that must be exceeded before an entry is deleted from the forwarding table.

6 Click *OK* to return to either the LAN1 or LAN2 screen where updates to the Mesh STP Configuration can be saved by clicking the *Apply* button.

7 Click *Cancel* to discard the changes made to the Mesh STP Configuration and return to the LAN1 or LAN2 screen. Once the Mesh STP Configuration is defined, the Access Point's radio can be configured for base and/or client bridge support.

Configuring a WLAN for Mesh Networking Support

Each Access Point comprising a particular mesh network is required to be a member of the same WLAN. Therefore, each base bridge, client bridge or repeater within the mesh network must use the same WLAN in order to share the same ESSID, radio designation, security policy, MU ACL and Quality of Service policy. If intending to use the Access Point for mesh networking support, Extreme Networks recommends configuring at least one WLAN (of the 16 WLANs available) specifically for mesh networking support.

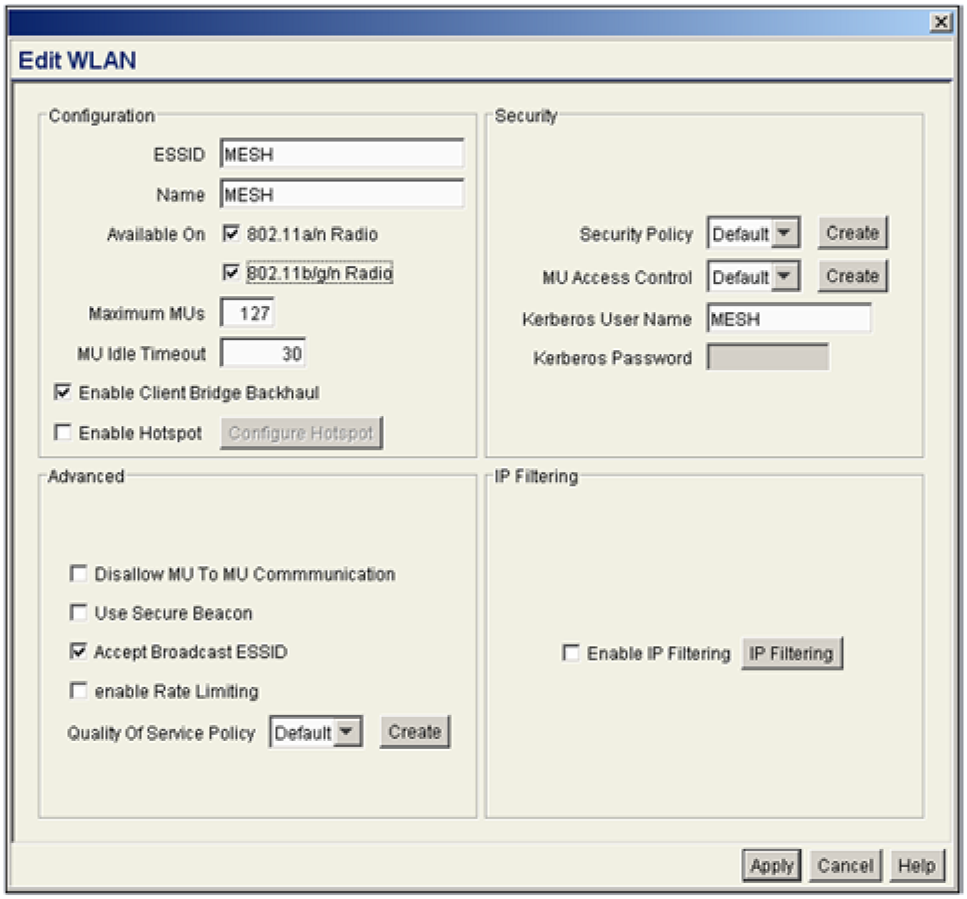
To define the attributes of the WLAN shared by the members of the mesh network:

1 Select *Network Configuration* > *Wireless* from the menu tree.

The *Wireless Configuration* screen displays with those existing WLANs displayed within the table.

2 Select the *Create* button to configure a new WLAN specifically to support mesh networking.

An existing WLAN can be modified (or used as is) for mesh networking support by selecting it from the list of available WLANs and clicking the *Edit* button.



Edit WLAN

Configuration

ESSID: MESH

Name: MESH

Available On: ☑ 802.11a/n Radio

☑ 802.11b/g/n Radio

Maximum MUs: 127

MU Idle Timeout: 30

☑ Enable Client Bridge Backhaul

□ Enable Hotspot

Security

Security Policy: Default

MU Access Control: Default

Kerberos User Name: MESH

Kerberos Password:

Advanced

□ Disallow MU To MU Commmunication

□ Use Secure Beacon

☑ Accept Broadcast ESSID

□ enable Rate Limiting

Quality Of Service Policy: Default

IP Filtering

□ Enable IP Filtering

3 Assign an *ESSID* and *Name* to the WLAN that each Access Point will share when using this WLAN within their mesh network.

Extreme Networks recommends assigning a unique name to a WLAN supporting a mesh network to differentiate it from WLANs defined for non mesh support. The name assigned to the WLAN is what is selected from the *Radio Configuration* screen for use within the mesh network.

NOTE

It is possible to have different ESSID and WLAN assignments within a single mesh network (one set between the Base Bridge and repeater and another between the repeater and Client Bridge). However, for ease of management and to not waste network bandwidth, Extreme Networks recommends using the same ESSID across the entire mesh network.

4 Use the *Available On* checkboxes to specify the Access Point radio(s) used with the target WLAN within the mesh network.

The Available On checkboxes are for making this WLAN available for base bridges or repeaters to connect to. The Available On checkbox should only be selected for a mesh WLAN if this target Access Point is to be configured as a base bridge or repeater on the radio. If the WLAN is to be defined for client bridge support only, the Available On checkbox should not be selected. Instead, it only needs to have the Enable Client Bridge Backhaul option selected.

5 Use the *Maximum MUs* field to define the number of MUs allowed to associate with this WLAN. This number should be defined based on the number of client bridge and repeaters within this mesh network. This value can be increased as the mesh network grows and devices are added.

Only advanced users should define the number of devices allowed to associate with the WLAN, as setting the value too low could restrict devices from joining an expanding mesh network, and setting it too high could prohibit other WLANs from granting access to the all the devices needed.

6 Select the *Enable Client Bridge Backhaul* checkbox to make this WLAN available in the *Mesh Network Name* drop-down menu within the *Radio Configuration* screen. Only WLANs defined for mesh networking support should have this checkbox selected, in order to keep the list of WLANs available (within the Radio Configuration screen) restricted to just WLANs configured specifically with mesh attributes.

7 Refer to the *Security Policy* drop-down menu to select the security policy used within this WLAN and mesh network.

A security policy for a mesh network should be configured carefully since the data protection requirements within a mesh network differ somewhat compared to a typical wireless LAN. *No Encryption* is a bad idea in a mesh network, since mesh networks are typically not guest networks, wherein public assess is more important than data protection. Extreme Networks also discourages user-based authentication schemes such as Kerberos and 802.1x EAP, as these authentication schemes are not supported within a mesh network.

If none of the existing policies are suitable, select the *Create* button to the right of the *Security Policy* drop-down menu and configure a policy suitable for the mesh network. For information on configuring a security using the authentication and encryption techniques available to the Access Point, see "Enabling Authentication and Encryption Schemes" on page 200.

8 ACL policies should be configured to allow or deny a range of MAC addresses from interoperating with the WLAN used with the mesh network. ACLs should be defined based on the client bridge and repeater (an Access Point defined as both a base and client bridge) association requirements within the mesh network.

For information on defining an ACL for use with the WLAN assigned to the mesh network, see "Configuring a WLAN Access Control List (ACL)" on page 153.

NOTE

The Kerberos User Name and Kerberos Password fields can be ignored, as Kerberos is not supported as a viable authentication scheme within a mesh network.

9 Select the *Disallow MU to MU Communication* checkbox to restrict MUs from interacting with each other both within this WLAN, as well as other WLANs.

Selecting this option could be a good idea, if restricting device "chatter" improves mesh network performance. If base bridges and client bridges are added at any given time to extent the coverage are of a mesh network, the data going back and forth amongst just those radios could be compromised by network interference. Adding mesh device traffic could jeopardize network throughput. If however, MU to MU communication is central to the organization (for example, scanners sharing data entry information) then this checkbox should remain unselected.

10 Select the *Use Secure Beacon* checkbox to not transmit the ESSID amongst the Access Points and devices within the mesh network. If a hacker tries to find an ESSID via an MU, the Access Point's ESSID does not display since the ESSID is not in the beacon. Extreme Networks recommends keeping the option enabled to reduce the likelihood of hacking into the WLAN.

11 Select the *Accept Broadcast ESSID* checkbox to associate an MU that has a blank ESSID (regardless of which ESSID the Access Point is currently using). Traffic within a mesh network probably consists of known devices, so you may want to leave the checkbox unselected and configure each MU with an ESSID. The default is selected. However, for WLANs used within a mesh network, Extreme Networks recommends unselecting this option as it would prevent the AP from answering to blank ESSID probes from other mobile units.

12 If there are certain requirements for the types of data proliferating the mesh network, select an existing policy or configure a new QoS policy best suiting the requirements of the mesh network. To define a new QoS policy, select the *Create* button to the right of the Quality Of Service Policy drop-down menu.

For detailed information on configuring a QoS policy, see "Setting the WLAN Quality of Service (QoS) Policy" on page 156.

13 Click *Apply* to save the changes made to the mesh network configured WLAN.

An Access Point radio is now ready to be configured for use with this newly created mesh WLAN.

Configuring the Access Point Radio for Mesh Support

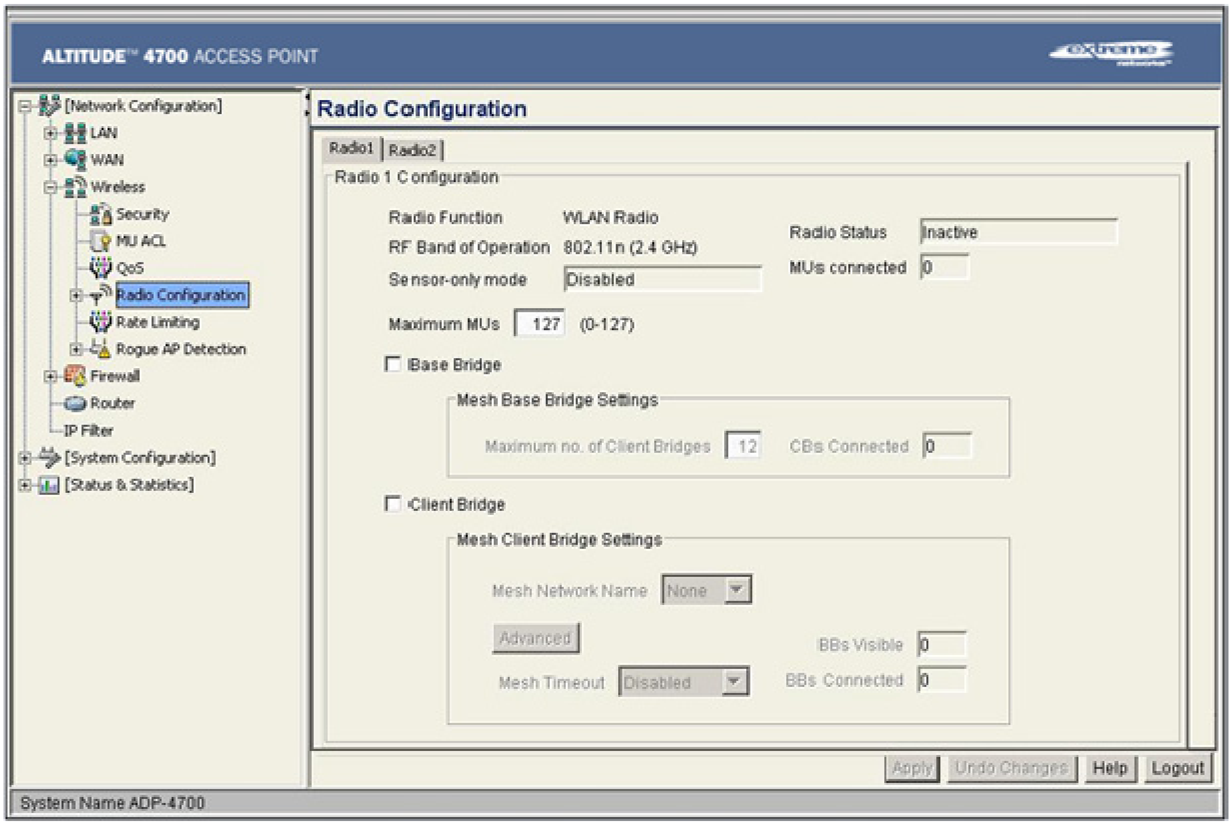
An Access Point radio intended for use within a mesh network requires configuration attributes unique from a radio intended for non-mesh support.This section describes how to configure an Access Point radio for mesh network support.

To configure the Access Point radio for mesh networking support:

NOTE

The dual-radio model Access Point affords users better optimization of the mesh network feature by allowing the Access Point to transmit to other Access Points (in base or client bridge mode) using one independent radio and transmit with its associated devices using the second independent radio.

1 Select *Network Configuration* > *Wireless* > *Radio Configuration* from the menu tree.



Radio Configuration

Radio 1 Configuration

Radio Function WLAN Radio
RF Band of Operation 802.11n (2.4 GHz)
Sensor-only mode Disabled
Radio Status Inactive
MUs connected 0
Maximum MUs 127 (0-127)

□ Base Bridge

Mesh Base Bridge Settings
Maximum no. of Client Bridges 12
CBs Connected 0

□ Client Bridge

Mesh Client Bridge Settings
Mesh Network Name None
BBs Visible 0
Mesh Timeout Disabled
BBs Connected 0

System Name ADP-4700

2 Refer to the *Radio Function* parameter to ensure the radio has been designated for WLAN Radio support.

Refer to *RF Band of Operation* parameter to ensure you are enabling the correct 802.11a/n or 802.11b/g/n radio. After the settings are applied within this Radio Configuration screen, the *Radio Status* and *MUs connected* values update. If this is an existing radio within a mesh network, these values update in real-time.

3 Select the *Base Bridge* checkbox to allow the Access Point radio to accept client bridge connections from other Access Points in client bridge mode. The base bridge is the acceptor of mesh network data from those client bridges within the mesh network and never the initiator.

CAUTION

A problem could arise if a Base Bridge's Indoor channel is not available on an Outdoor Client Bridge's list of available channels. As long as an Outdoor Client Bridge has the Indoor Base Bridge channel in its available list of channels, it can associate to the Base Bridge.

4 If the Base Bridge checkbox has been selected, use the *Max# Client Bridges* parameter to define the client bridge load on a particular base bridge.

The maximum number of client bridge connections per Access Point radio is 12, with 24 representing the maximum for dual-radio models.

CAUTION

An Access Point in Base Bridge mode logs out whenever a Client Bridge associates to the Base Bridge over the LAN connection. This problem is not experienced over the Access Point's WAN connection. If this situation is experienced, log-in to the Access Point again.

Once the settings within the Radio Configuration screen are applied (for an initial deployment), the current number of client bridge connections for this specific radio displays within the *CBs Connected* field. If this is an existing radio within a mesh network, this value updates in real-time.

5 Select the *Client Bridge* checkbox to enable the Access Point radio to initiate client bridge connections with other mesh network supported Access Points radios on the same WLAN.

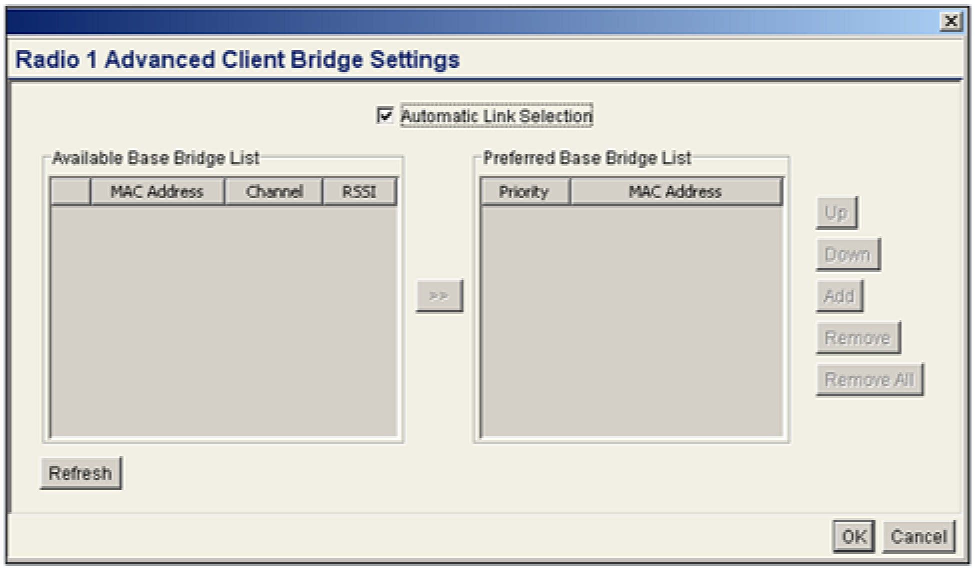
If the Client Bridge checkbox has been selected, use the *Mesh Network Name* drop-down menu to select the WLAN (ESS) the client bridge uses to establish a wireless link. The default setting, is (WLAN1). Extreme Networks recommends creating (and naming) a WLAN specifically for mesh networking support to differentiate the Mesh supported WLAN from non-Mesh supported WLANs. For more information, see *"Configuring a WLAN for Mesh Networking Support" on page 583*

Once the settings within the Radio Configuration screen are applied (for an initial deployment), the current number of base bridges visible to the radio displays within the *BBs Visible* field, and the number of base bridges currently connected to the radio displays within the *BBs Connected* field. If this is an existing radio within a mesh network, these values update in real-time.

NOTE

Ensure you have verified the radio configuration for both Radio 1 and Radio 2 before saving the existing settings and exiting the Radio Configuration screen.

6 Click the *Advanced* button to define a prioritized list of Access Points to define mesh connection links.



Radio 1 Advanced Client Bridge Settings

☑ Automatic Link Selection

7 Select the *Automatic Link Selection* checkbox to allow the Access Point to select the links used by the client bridge to populate the mesh network. Selecting this checkbox prohibits the user from selecting

the order base bridges are added to the mesh network when one of the three associated base bridges becomes unavailable.

NOTE

Auto link selection is based on the RSSI and load. The client bridge will select the best available link when the Automatic Link Selection checkbox is selected. Extreme Networks recommends you do not disable this option, as (when enabled) the Access Point will select the best base bridge for connection.

8 Refer to the *Available Base Bridge List* to view devices located by the Access Point using the WLAN selected from the Radio Configuration screen. Refer the following for information on located base bridges:

MAC	The MAC field displays the factory set hard-coded MAC address that serves as a device identifier.
RSSI	The Relative Signal Strength Indicator (RSSI) displays the located device's signal strength with the associated Access Point in client bridge mode. Use this information as criteria on whether to move a particular device from the available list to the preferred list.
CHANN	The CHANN displays the name of the channel that both the Access Point and base bridge use. A client bridge can only connect to Access Points (Base Bridges) on the same channel. If the user selects multiple base bridges on different channels, the Access Point will only be able to connect to those bridges on the same channel and the others will not be able to join this particular mesh network.

9 Click *Refresh* at any time to update the list of available Base Bridge devices available to the Access Point.

10 Use the >> button to move a selected base bridge MAC address from Available Base Bridge List.

11 Refer to the *Preferred Base Bridge List* for a prioritized list of base bridges the mesh network's client bridge uses to extend the mesh network's coverage area and potentially provide redundant links. If a device does not appear on the Available Base Bridge List, there is no way it can be moved to Preferred Base Bridge List as the device has not yet been *seen*. However, if you know the MAC Address corresponding to that Base Bridge, you can add that to the Preferred List using the add button.

12 Highlight a MAC address from the Preferred Base Bridge List and click the *Up* button to assign that device's MAC address a higher priority and a greater likelihood of joining the mesh network if an association with another device is lost.

If a MAC address is not desirable as others but still worthy of being on the preferred list, select it, and click the *Down* button to decrease its likelihood of being selected as a member of the mesh network.

13 If a device MAC address is on the Preferred Base Bridge List and constitutes a threat as a potential member of the mesh network (poor RSSI etc.), select it and click the *Remove* button to exclude it from the preferred list.

If all of the members of the Preferred Base Bridge List constitute a risk as a member of the mesh network, click the *Remove All* button. This is not recommended unless the preferred list can be re-populated with more desirable device MAC addresses from the Available Base Bridge List.

14 Click *Ok* to return to the Radio Configuration screen. Within the Radio Configuration screen, click *Apply* to save any changes made within the Advanced Client Bridge Settings screen.

15 Click *Cancel* to undo any changes made within the Advanced Client Bridge Settings screen. This reverts all settings for the screen to the last saved configuration.

16 If using a dual-radio model Access Point, refer to the *Mesh Timeout* drop-down menu (from within the Radio Configuration screen) to define whether one of the Access Point's radio's beacons on an existing WLAN or if a client bridge radio uses an uplink connection. The following drop-down menu options are available:

Disabled	When disabled, both radios are up at boot time and beaconing. If one radio (radio 1) does not have a mesh connection, the other radio (radio 2) is not affected. Radio 2 continues to beacon and associate MUs, but MU's can only communicate amongst themselves using the Access Point. Disabled is the default value.
Upload Detect	When Uplink Detect is selected, the Access Point only boots up the radio configured as a client bridge. The Access Point boots up the second radio as soon as the first mesh connection is established. However, if the client bridge radio loses its uplink connection, the second radio shuts down immediately.
Enabled	If the mesh connection is down on one radio (radio 1), the other radio (radio 2) is brought down and stops beaconing after the timeout period (45 seconds). This allows the client bridge (radio 1) to roam without dropping the MUs associated to radio 2. The disadvantage is that radio 2 may beacon for the 45 second timeout period and have to drop associated MUs because radio 1 could not establish its uplink.

NOTE

The Mesh Time Out variable overrides the Ethernet Port Time Out (EPTO) setting on the LAN page when the Access Point is in bridge mode. As long as the mesh is down, the Access Point acts in accordance to the Mesh Time Out setting regardless of the state of the Ethernet. However, if the Ethernet goes down and the mesh link is still up, the EPTO takes effect.

17 Click *Apply* to save any changes to the Radio Configuration screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

CAUTION

When defining a Mesh configuration and changes are saved, the mesh network temporarily goes down. The mesh network is unavailable because the Access Point radio goes down when applying the changes. This can be problematic for users making changes within a deployed mesh network. If updating the mesh network using a LAN connection, the Access Point applet loses connection and the connection must be re-instated. If updating the mesh network using a WAN connection, the applet does not lose connection, but the mesh network is unavailable until the changes have been applied.

18 Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Radio Configuration screen to the last saved configuration.

19 Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Once the target radio has been enabled from the *Radio Configuration* screen, configure the radio's properties by selecting it from the menu tree.

For additional information on configuring the Access Point's radio, see "Configuring the 802.11a/n or 802.11b/g/n Radio" on page 174. For two fictional deployment scenarios, see "Mesh Network Deployment - Quick Setup" on page 590.

Mesh Network Deployment - Quick Setup

This section provides instructions on how to quickly setup and demonstrate mesh functionality using three Access Points. Two following two deployment scenarios will be addressed:

- *Scenario 1*—Two base bridges (redundant) and one client bridge
- *Scenario 2*—A two hop mesh network with a base bridge, repeater (combined base bridge and client bridge mode) and a client bridge.

Scenario 1 - Two Base Bridges and One Client Bridge

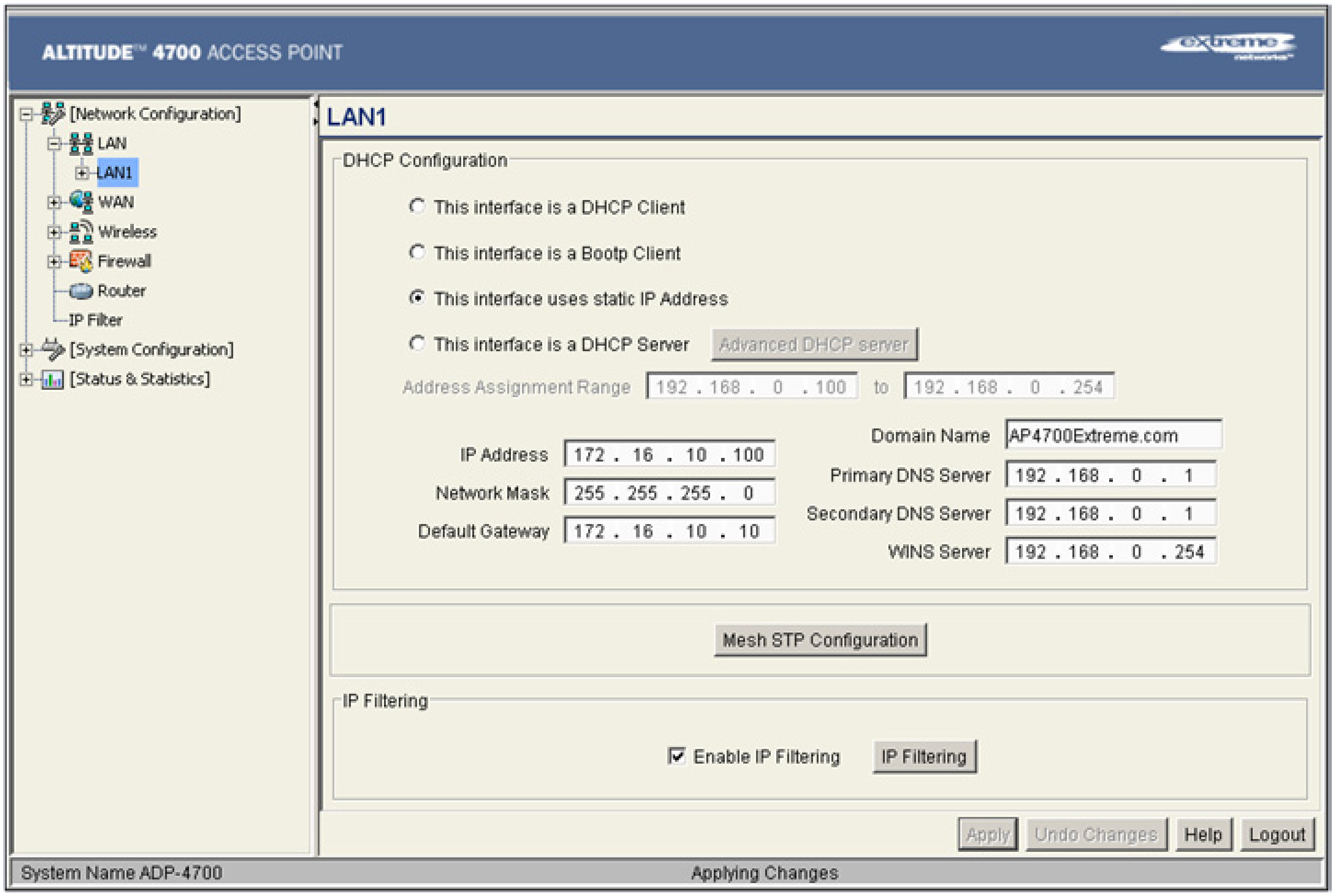
In scenario 1, the following three Access Point configurations will be deployed within the mesh network:

- AP#1—An active base bridge
- AP#2—A redundant base bridge
- AP#3—A client bridge connecting to both AP#1 and AP#2 simultaneously.

AP#1 and AP#2 will be configured somewhat the same. However there are some important (yet subtle) differences. Therefore, the configuration of each Access Point will be described separately.

Configuring AP#1:

1 Provide a known IP address for the LAN1 interface.



LAN1

DHCP Configuration

○ This interface is a DHCP Client

○ This interface is a Bootp Client

● This interface uses static IP Address

○ This interface is a DHCP Server

Address Assignment Range 192 . 168 . 0 . 100 to 192 . 168 . 0 . 254

IP Address 172 . 16 . 10 . 100

Network Mask 255 . 255 . 255 . 0

Default Gateway 172 . 16 . 10 . 10

Domain Name AP4700Extreme.com

Primary DNS Server 192 . 168 . 0 . 1

Secondary DNS Server 192 . 168 . 0 . 1

WINS Server 192 . 168 . 0 . 254

IP Filtering

☑ Enable IP Filtering

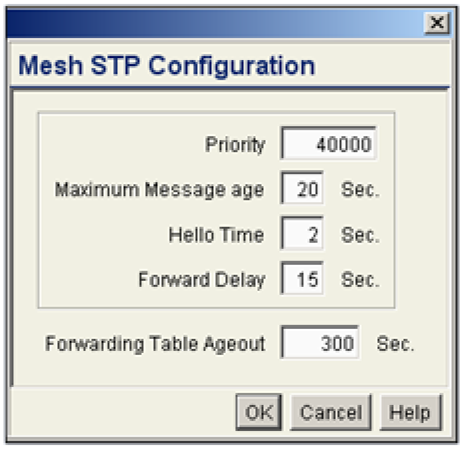
System Name ADP-4700

Applying Changes

NOTE

Enable the LAN1 Interface of AP#1 as a DHCP Server if you intend to associate MUs and require them to obtain an IP address via DHCP.

2 Assign a Mesh STP Priority of 40000 to LAN1 Interface.



Mesh STP Configuration

Priority 40000

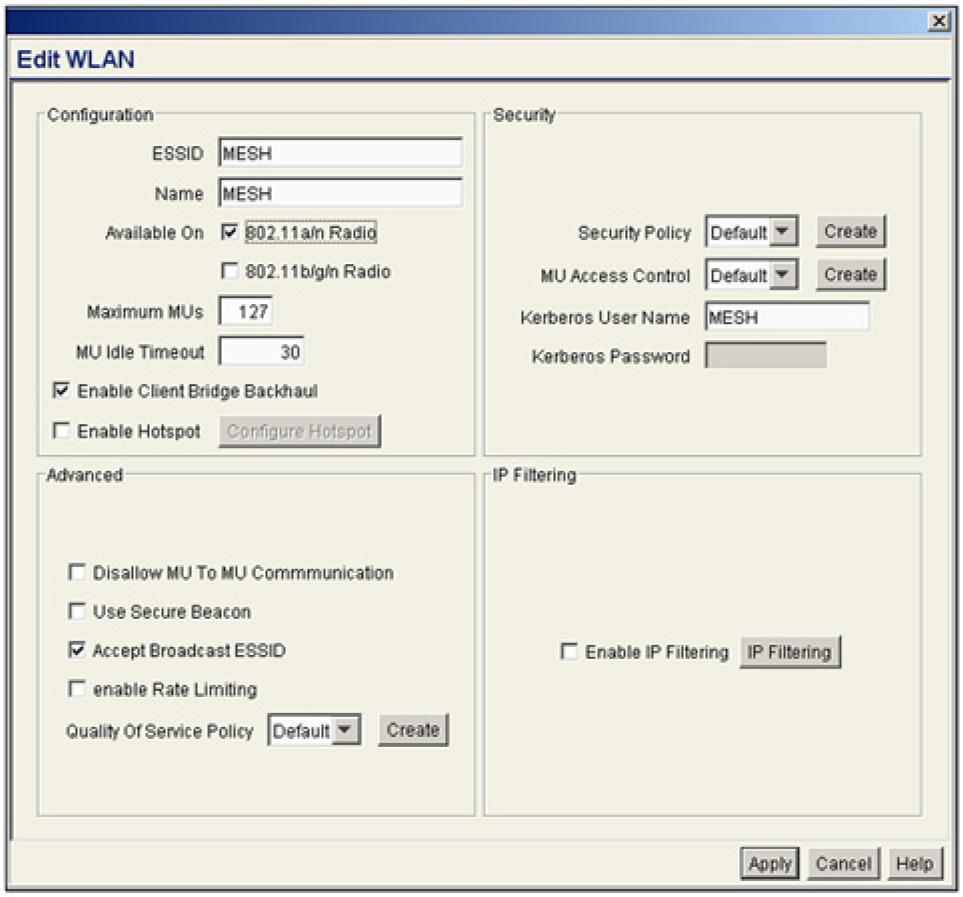
Maximum Message age 20 Sec.

Hello Time 2 Sec.

Forward Delay 15 Sec.

Forwarding Table Ageout 300 Sec.

3 Define a mesh supported WLAN.



Edit WLAN

Configuration

ESSID MESH

Name MESH

Available On ☑ 802.11a/n Radio

□ 802.11b/g/n Radio

Maximum MUs 127

MU Idle Timeout 30

☑ Enable Client Bridge Backhaul

□ Enable Hotspot

Security

Security Policy Default

MU Access Control Default

Kerberos User Name MESH

Kerberos Password

Advanced

□ Disallow MU To MU Commmunication

□ Use Secure Beacon

☑ Accept Broadcast ESSID

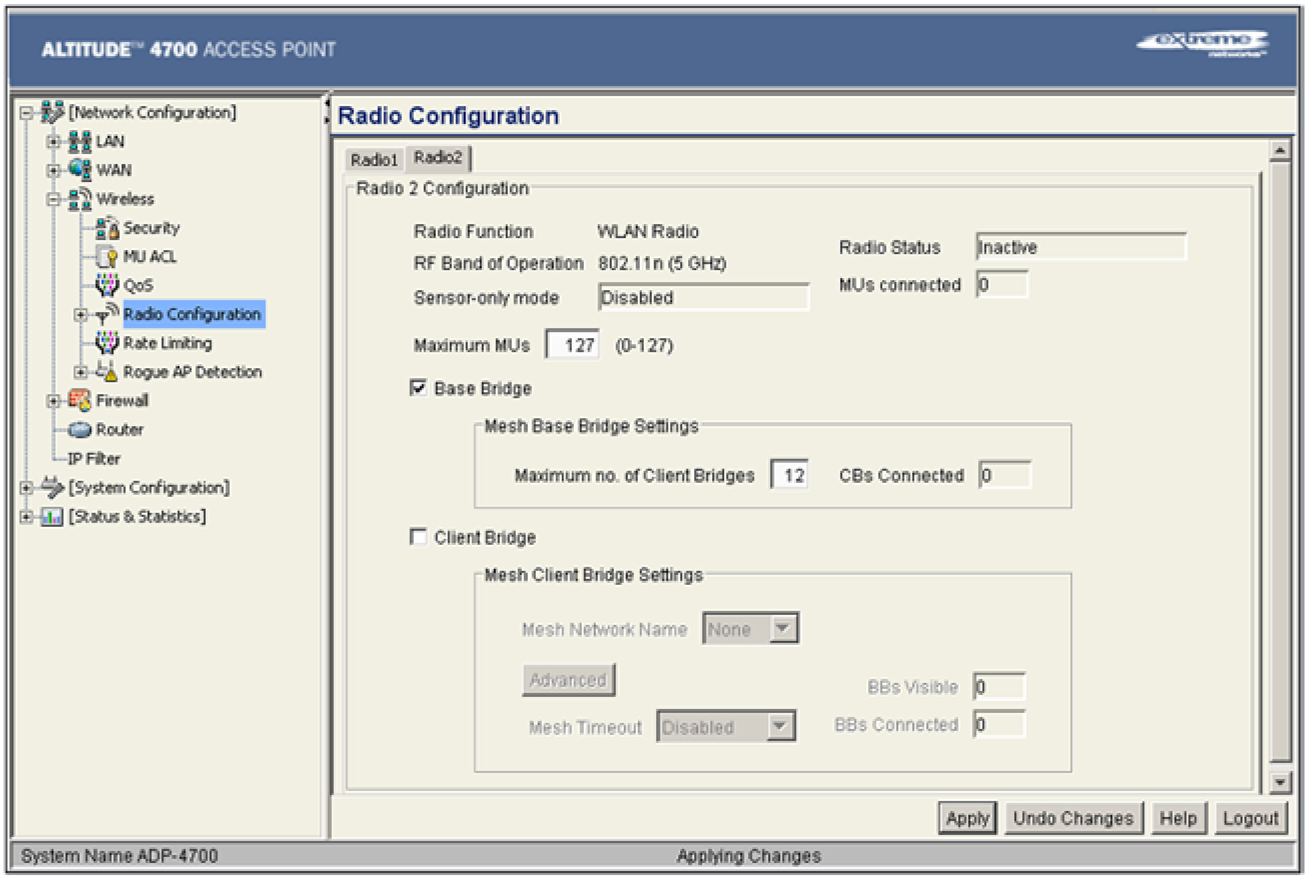
□ enable Rate Limiting

Quality Of Service Policy Default

IP Filtering

□ Enable IP Filtering

4 Enable base bridge functionality on the 802.11a/n radio (Radio 2).



Radio Configuration

Radio 2 Configuration

Radio Function WLAN Radio

RF Band of Operation 802.11n (5 GHz)

Sensor-only mode Disabled

Radio Status Inactive

MUs connected 0

Maximum MUs 127 (0-127)

☑ Base Bridge

Mesh Base Bridge Settings

Maximum no. of Client Bridges 12

CBs Connected 0

☐ Client Bridge

Mesh Client Bridge Settings

Mesh Network Name None

Advanced

BBs Visible 0

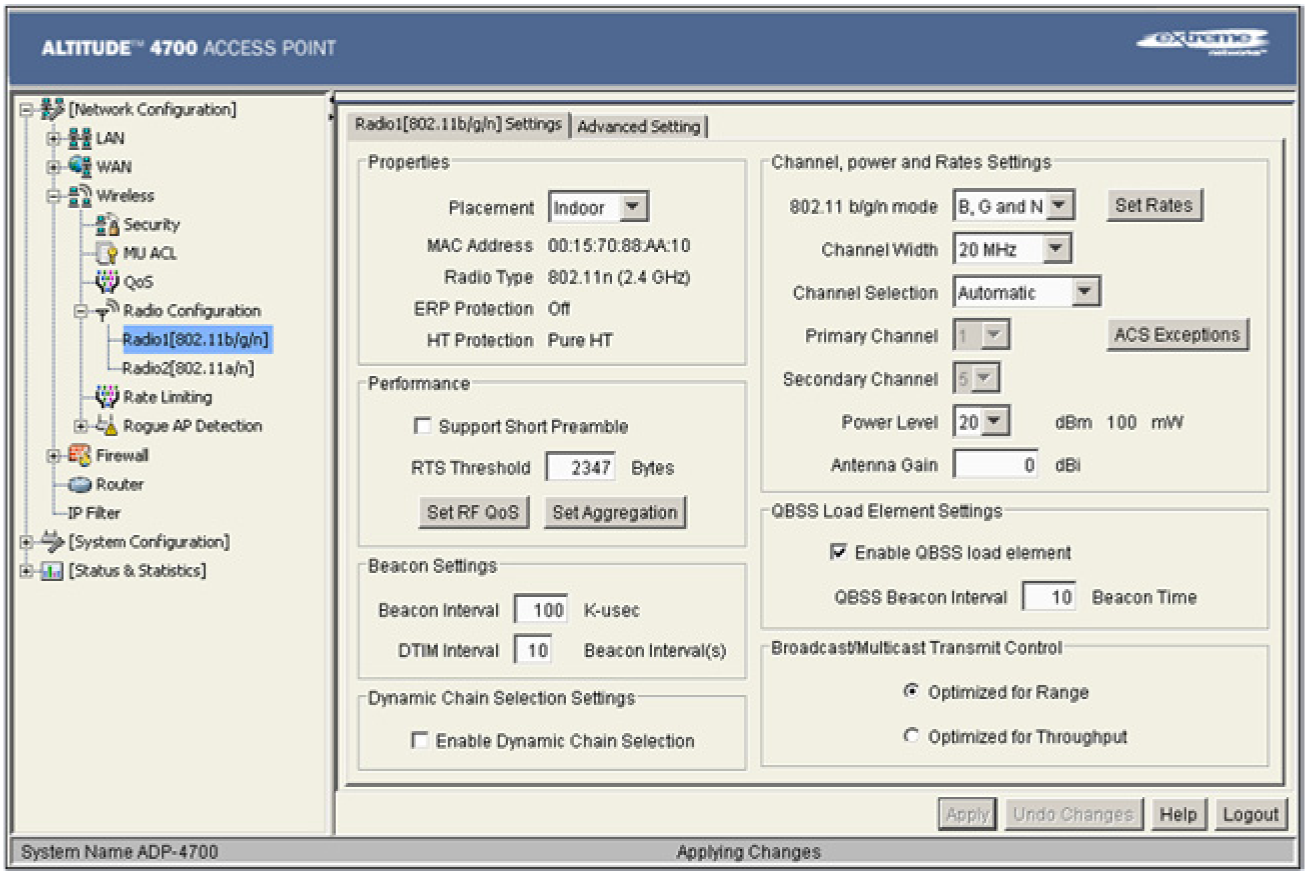
Mesh Timeout Disabled

BBs Connected 0

System Name ADP-4700

Applying Changes

5 Define a channel of operation for the 802.11a/n radio.



Properties

Placement: Indoor
MAC Address: 00:15:70:88:AA:10
Radio Type: 802.11n (2.4 GHz)
ERP Protection: Off
HT Protection: Pure HT

Performance

☐ Support Short Preamble
RTS Threshold: 2347 Bytes

Beacon Settings

Beacon Interval: 100 K-usec
DTIM Interval: 10 Beacon Interval(s)

Dynamic Chain Selection Settings

☐ Enable Dynamic Chain Selection

Channel, power and Rates Settings

802.11 b/g/n mode: B, G and N
Channel Width: 20 MHz
Channel Selection: Automatic
Primary Channel: 1
Secondary Channel: 5
Power Level: 20 dBm 100 mW
Antenna Gain: 0 dBi

QBSS Load Element Settings

☑ Enable QBSS load element
QBSS Beacon Interval: 10 Beacon Time

Broadcast/Multicast Transmit Control

● Optimized for Range
○ Optimized for Throughput

System Name ADP-4700
Applying Changes

6 If needed, create another WLAN mapped to the 802.11b/g/n radio if 802.11b/g/n support is required for MUs on that 802.11 band.

Configuring AP#2

AP#2 can be configured the same as AP#1 with the following exceptions:

- Assign an IP Address to the LAN1 Interface different than that of AP#1
- Assign a higher Mesh STP Priority 50000 to the AP#2 LAN1 Interface.

NOTE

In a typical deployment, each base bridge can be configured for a Mesh STP Priority of 50000. In this example, different values are used to force AP#1 to be the forwarding link since it's a small mesh network (of only three APs) with AP within close proximity of one another.

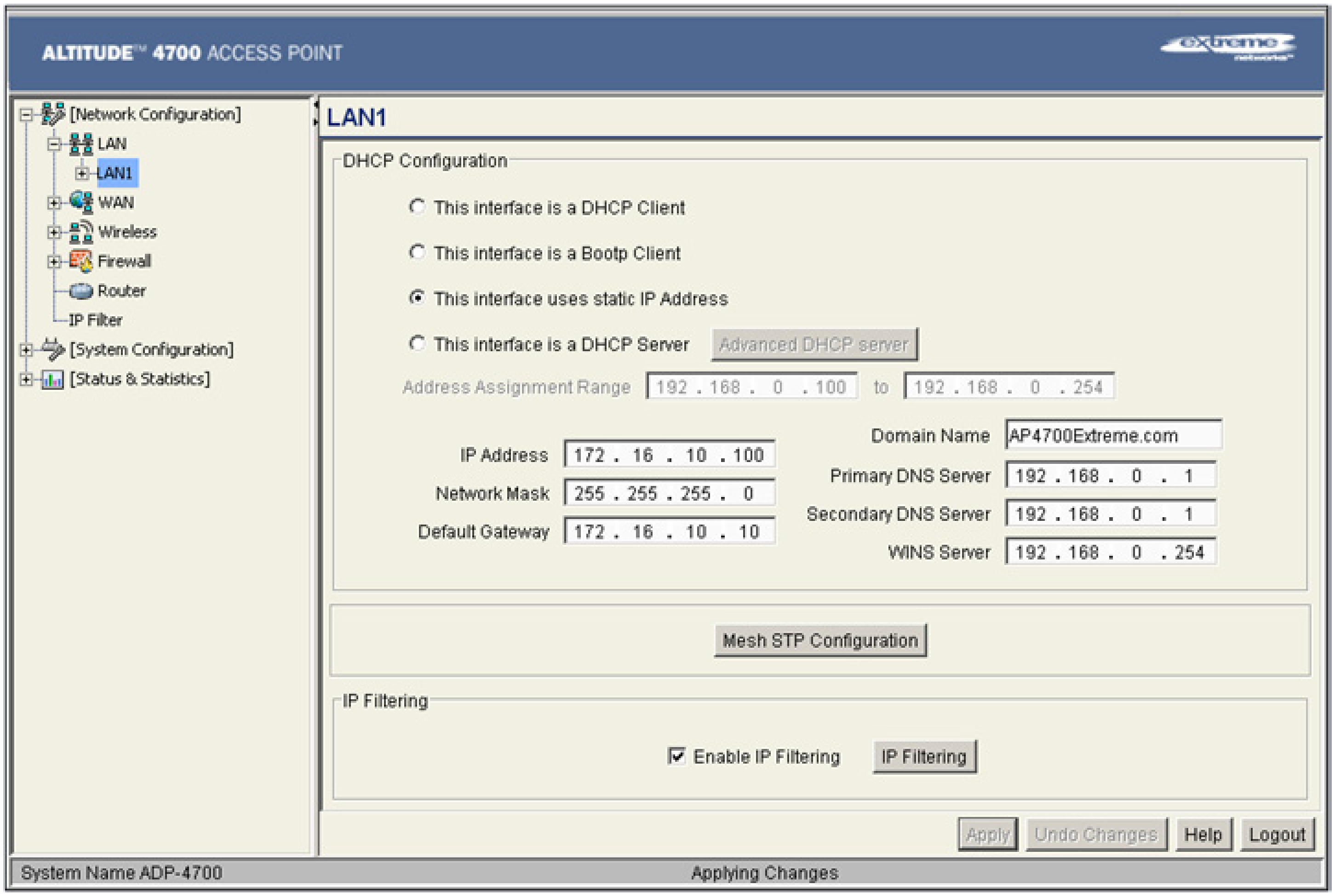
NOTE

Ensure AP#1 and AP#2 use the same channel for each 802.11a/n radio, or the APs will not be able to “hear” each other over different channels.

Configuring AP#3

To define the configuration for AP#3 (a client bridge connecting to both AP#1 and AP#2 simultaneously):

1 Provide a known IP address for the LAN1 interface.



LAN1

DHCP Configuration

○ This interface is a DHCP Client

○ This interface is a Bootp Client

● This interface uses static IP Address

○ This interface is a DHCP Server

Address Assignment Range 192 . 168 . 0 . 100 to 192 . 168 . 0 . 254

IP Address 172 . 16 . 10 . 100

Network Mask 255 . 255 . 255 . 0

Default Gateway 172 . 16 . 10 . 10

Domain Name AP4700Extreme.com

Primary DNS Server 192 . 168 . 0 . 1

Secondary DNS Server 192 . 168 . 0 . 1

WINS Server 192 . 168 . 0 . 254

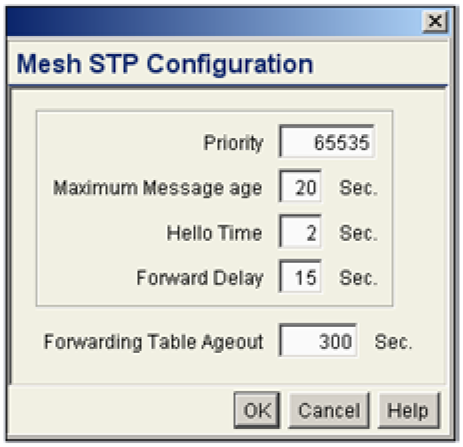
IP Filtering

☑ Enable IP Filtering

System Name ADP-4700

Applying Changes

2 Assign the maximum value (65535) for the Mesh STP Priority.



Mesh STP Configuration

Priority 65535

Maximum Message age 20 Sec.

Hello Time 2 Sec.

Forward Delay 15 Sec.

Forwarding Table Ageout 300 Sec.

3 Create a mesh supported WLAN with the *Enable Client Bridge Backhaul* option selected.

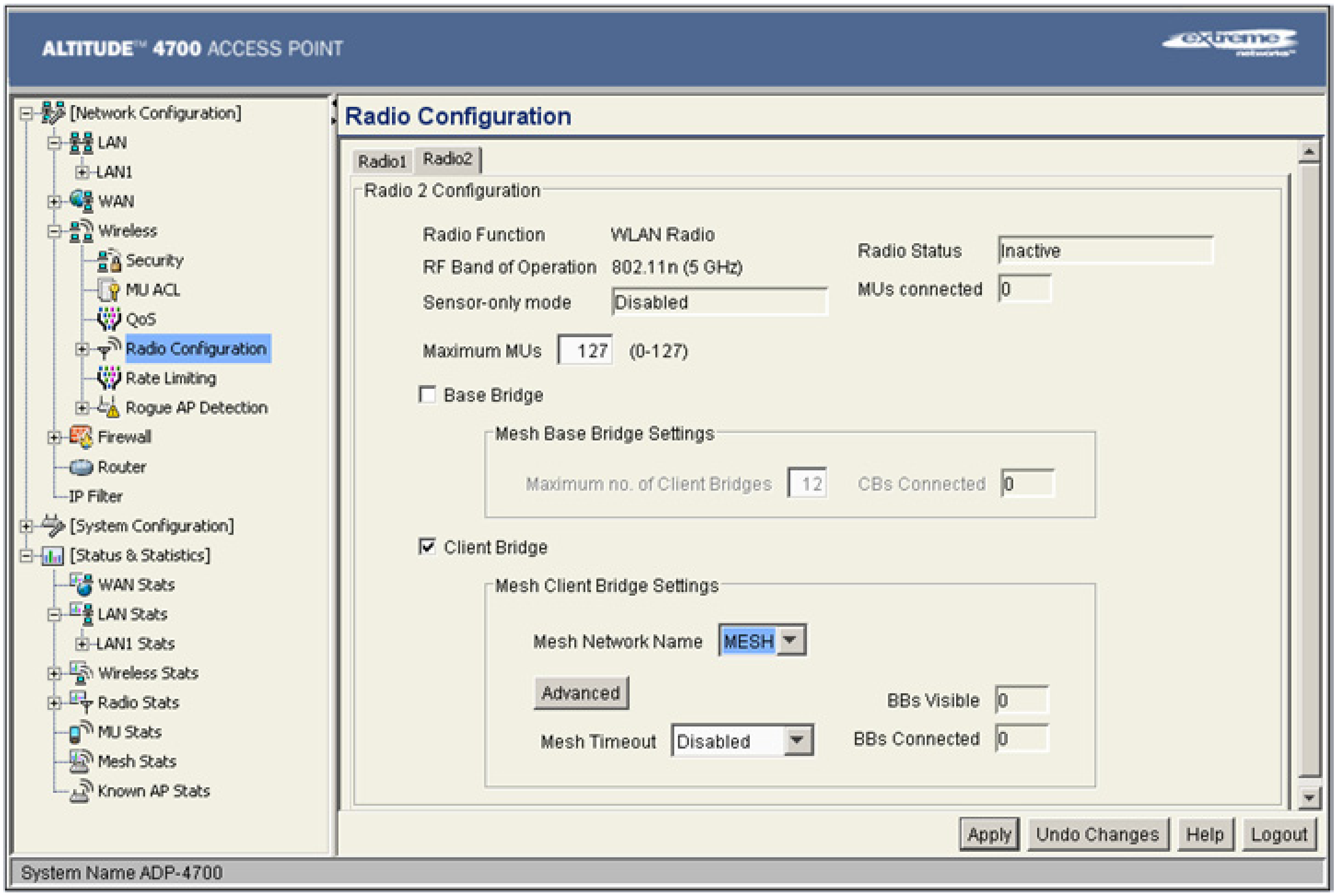
NOTE

This WLAN should not be mapped to any radio. Therefore, leave both of the “Available On” radio options unselected.

4 Select the *Client Bridge* checkbox to enable client bridge functionality on the 802.11a/n radio. Use the *Mesh Network Name* drop-down menu to select the name of the WLAN created in step 3.

NOTE

You don't need to configure channel settings on the client bridge (AP#3). It automatically finds the base bridges (AP#1 and AP#2) and uses the channel assigned to them.



Radio Configuration

Radio 2 Configuration

Radio Function: WLAN Radio
RF Band of Operation: 802.11n (5 GHz)
Sensor-only mode: Disabled
Radio Status: Inactive
MUs connected: 0
Maximum MUs: 127 (0-127)

☐ Base Bridge

Mesh Base Bridge Settings
Maximum no. of Client Bridges: 12
CBs Connected: 0

☑ Client Bridge

Mesh Client Bridge Settings
Mesh Network Name: MESH
Mesh Timeout: Disabled
BBs Visible: 0
BBs Connected: 0

System Name ADP-4700

5 If needed, create another WLAN mapped to the 802.11b/g/n radio if 802.11b/g/n support is required for MUs on that 802.11 band.

Verifying Mesh Network Functionality for Scenario #1

You now have a three AP mesh network ready to demonstrate. Associate a single MU on each AP WLAN configured for 802.11b/g/n radio support. Once completed, pass traffic among the three APs comprising the mesh network.

Scenario 2 - Two Hop Mesh Network with a Base Bridge Repeater and a Client Bridge

By default, the mesh algorithm runs an automatic link selection algorithm to determine the best possible active and redundant links. If member APs are not far apart (in physical distance), the algorithm intelligently chooses a single hop link to forward data. To force APs to use multiple hops for demonstrations, use manual links.

In scenario 2, the following three AP configurations comprise the mesh network:

- AP#1 is a base bridge.
- AP#2 is a repeater (client bridge/base bridge combination).
- AP#3 is a client bridge.

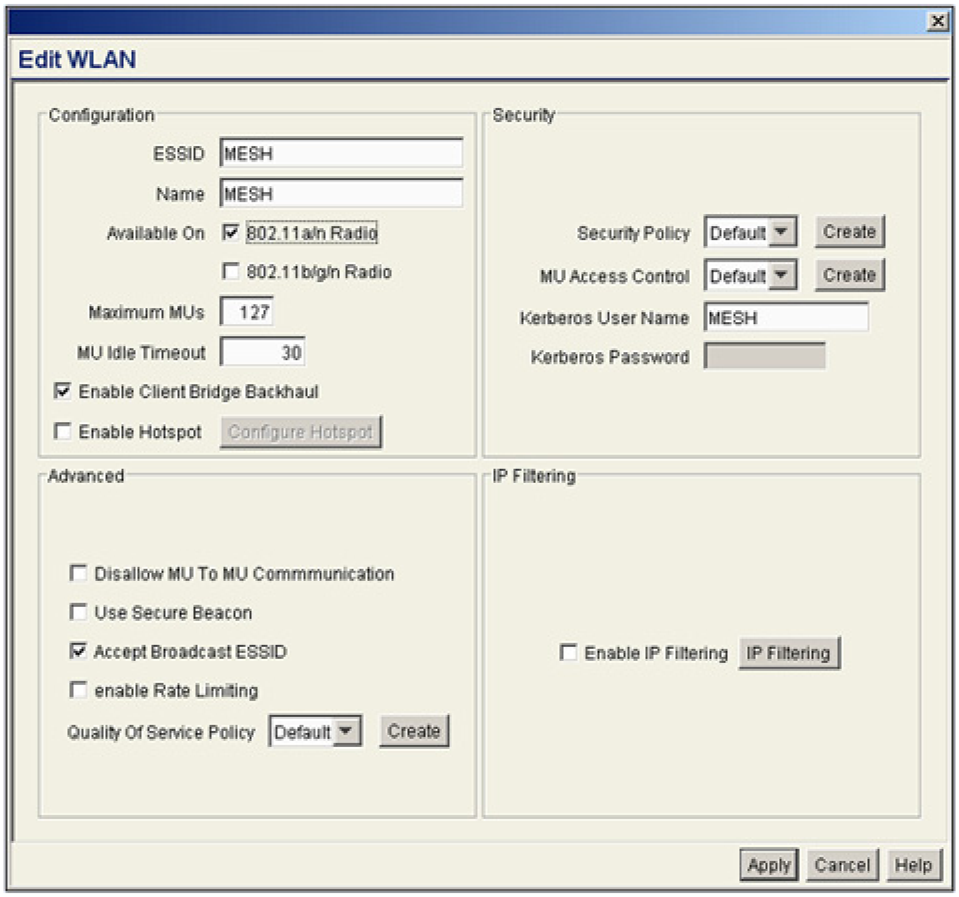
Configuring AP#1

The setup of AP#1 within this usage scenario is exactly the same as the AP#1 configuration within "Scenario 1 - Two Base Bridges and One Client Bridge" for step by step instructions for configuring AP#1, see "Configuring AP#1:" on page 591. Once completed, return to "Configuring AP#2" on page 598 within this section.

Configuring AP#2

AP#2 requires the following modifications from AP#2 in the previous scenario to function in base bridge/client bridge repeater mode.

1 Enable client bridge backhaul on the mesh supported WLAN.



Edit WLAN

Configuration

ESSID MESH

Name MESH

Available On ☑ 802.11a/n Radio

□ 802.11b/g/n Radio

Maximum MUs 127

MU Idle Timeout 30

☑ Enable Client Bridge Backhaul

□ Enable Hotspot

Security

Security Policy Default

MU Access Control Default

Kerberos User Name MESH

Kerberos Password

Advanced

□ Disallow MU To MU Commmunication

□ Use Secure Beacon

☑ Accept Broadcast ESSID

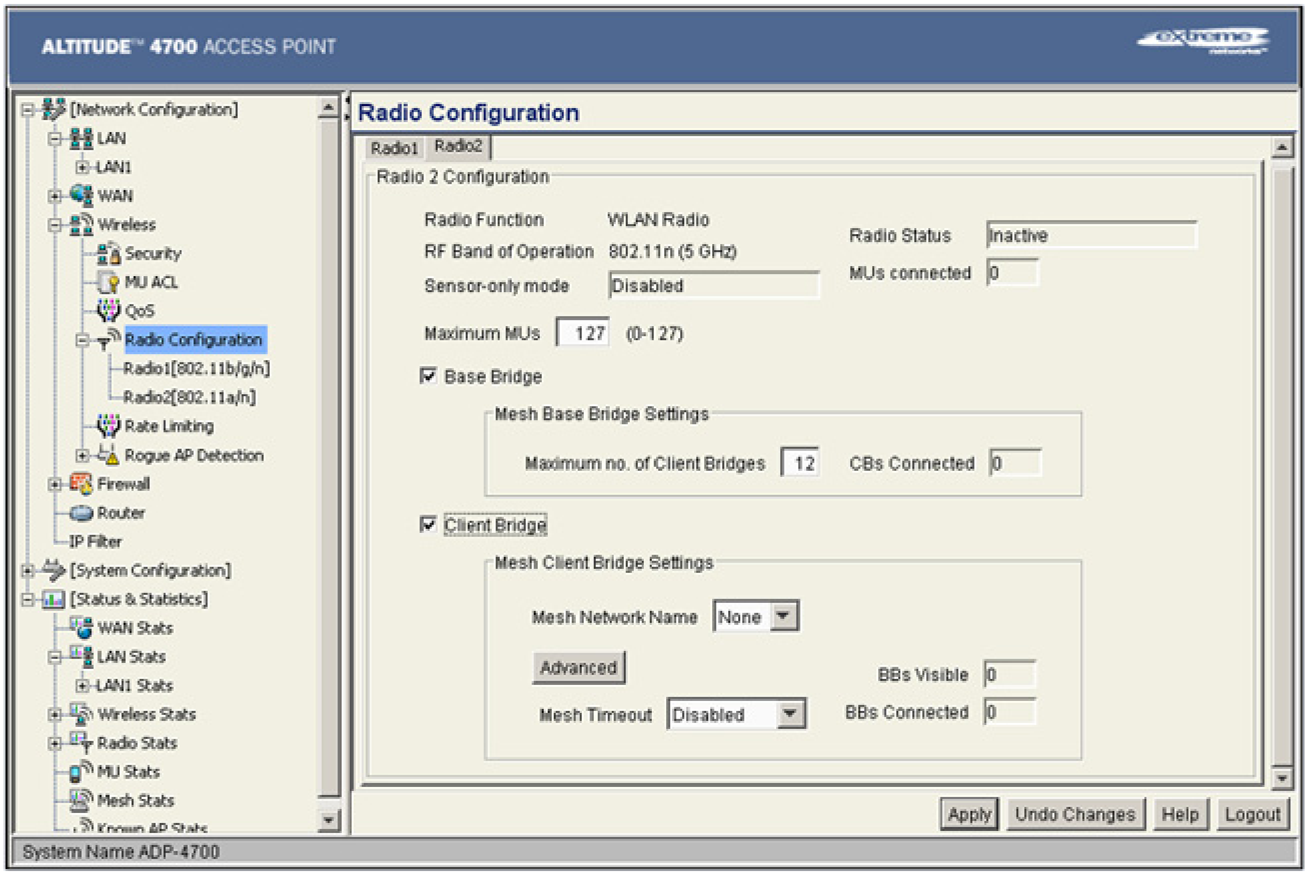
□ enable Rate Limiting

Quality Of Service Policy Default

IP Filtering

□ Enable IP Filtering

2 Enable client and base bridge functionality on the 802.11a/n radio



Radio Configuration

Radio 2 Configuration

Radio Function: WLAN Radio
RF Band of Operation: 802.11n (5 GHz)
Sensor-only mode: Disabled
Radio Status: Inactive
MUs connected: 0
Maximum MUs: 127 (0-127)

☑ Base Bridge

Mesh Base Bridge Settings
Maximum no. of Client Bridges: 12
CBs Connected: 0

☑ Client Bridge

Mesh Client Bridge Settings
Mesh Network Name: None
BBs Visible: 0
Mesh Timeout: Disabled
BBs Connected: 0

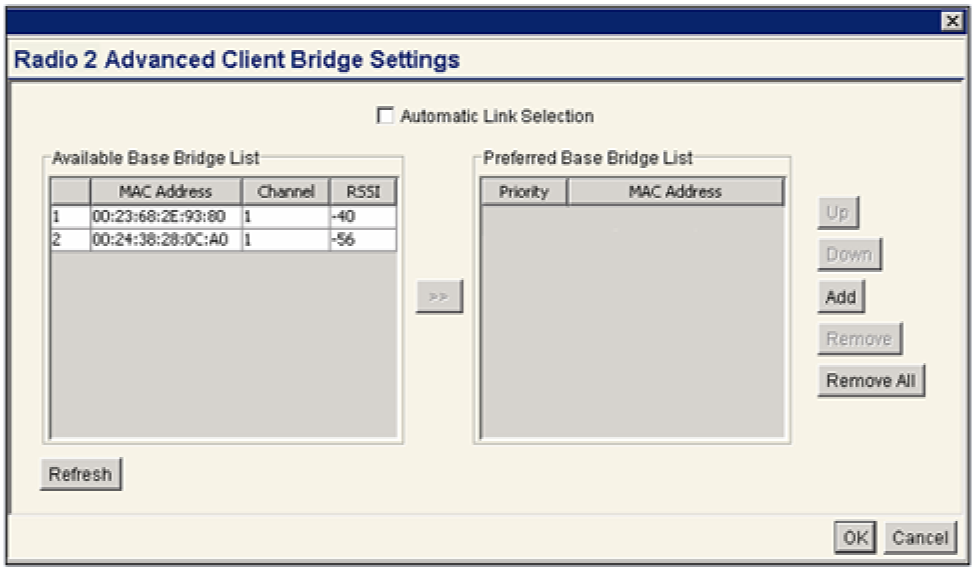
System Name ADP-4700

Configuring AP#3

To define AP #3's configuration:

1 The only change needed on AP#3 (with respect to the configuration used in scenario #1), is to disable the *Auto Link Selection* option.

Click the *Advanced* button within the *Mesh Client Bridge Settings* field.



Radio 2 Advanced Client Bridge Settings

□ Automatic Link Selection

Available Base Bridge List

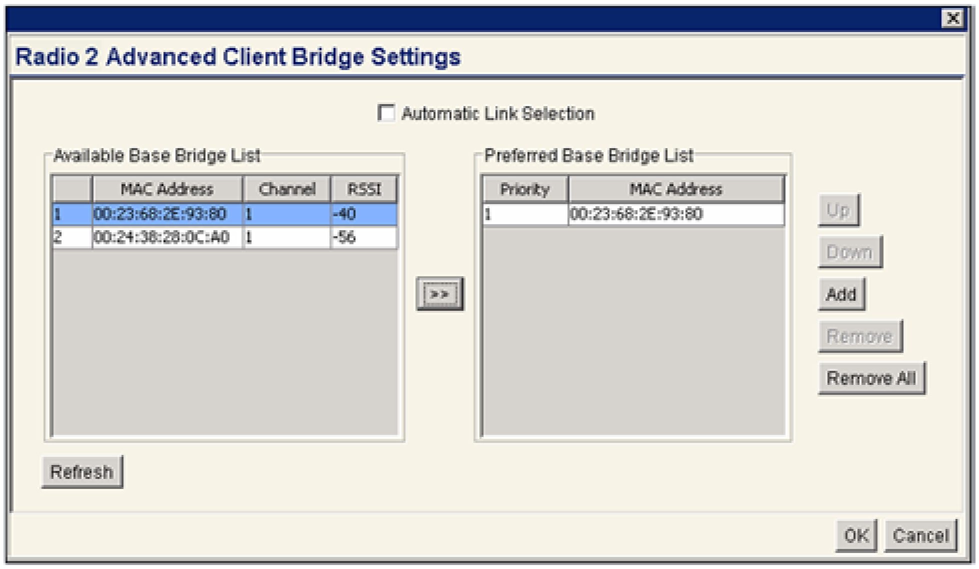
	MAC Address	Channel	RSSI
1	00:23:68:2E:93:80	1	-40
2	00:24:38:28:0C:A0	1	-56

Preferred Base Bridge List

Priority	MAC Address

2 Add the 802.11a/n Radio MAC Address.

In scenario #2, the mesh WLAN is mapped to BSS1 on the 802.11a/n radio if each AP. The Radio MAC Address (the BSSID#1 MAC Address) is used for the AP#2 Preferred Base Bridge List. Ensure both the AP#1 and AP#2 Radio MAC Addresses are in the Available Base Bridge List. Add the AP#2 MAC Address into the Preferred Base Bridge List.



Radio 2 Advanced Client Bridge Settings

□ Automatic Link Selection

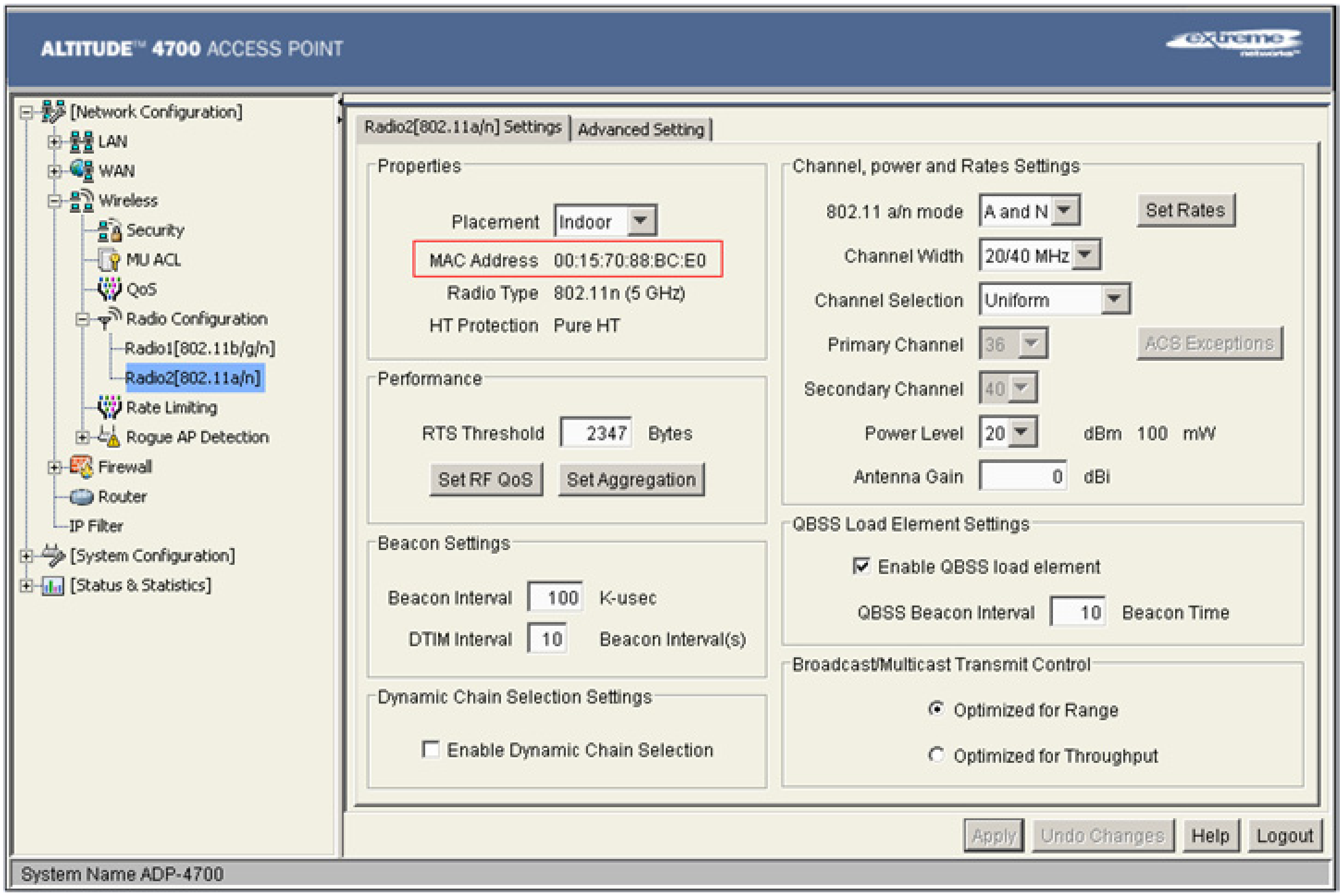
Available Base Bridge List

	MAC Address	Channel	RSSI
1	00:23:68:2E:93:80	1	-40
2	00:24:38:28:0C:A0	1	-56

Preferred Base Bridge List

Priority	MAC Address
1	00:23:68:2E:93:80

3 Determine the Radio MAC Address and BSSID MAC Addresses.



Properties

Placement: Indoor

MAC Address: 00:15:70:88:BC:E0

Radio Type: 802.11n (5 GHz)

HT Protection: Pure HT

Performance

RTS Threshold: 2347 Bytes

Beacon Settings

Beacon Interval: 100 K-usec

DTIM Interval: 10 Beacon Interval(s)

Dynamic Chain Selection Settings

☐ Enable Dynamic Chain Selection

Channel, power and Rates Settings

802.11 a/n mode: A and N

Channel Width: 20/40 MHz

Channel Selection: Uniform

Primary Channel: 36

Secondary Channel: 40

Power Level: 20 dBm 100 mW

Antenna Gain: 0 dBi

QBSS Load Element Settings

☑ Enable QBSS load element

QBSS Beacon Interval: 10 Beacon Time

Broadcast/Multicast Transmit Control

● Optimized for Range

○ Optimized for Throughput

System Name ADP-4700

Verifying Mesh Network Functionality for Scenario #2

You now have a three AP demo multi-hop mesh network ready to demonstrate. Associate an MU on the WLANs configured on the 802.11b/g/n radio for each AP and pass traffic among the members of the mesh network.

Mesh Networking Frequently Asked Questions

The following scenarios represent issues that could be encountered and resolved when defining an Access Point supported mesh configuration:

Mesh Deployment Issue 1 - Client Bridge can only connect to one of two Base Bridges

You have two Access Points configured as base bridges (AP1, AP2) and one Access Point defined as a as a client bridge (AP3). However, the client bridge is able to connect to only one of the base bridges.

Resolution:

Check the mesh backhaul radio channel configuration on both base bridges (AP1, AP2). They need to use the same channel so the client bridge can connect to both simultaneously.

Mesh Deployment Issue 2 - Faulty Client Bridge Connectivity

You have configured three Access Points in mesh mode; one base bridge (AP1), one client bridge/ base bridge (AP2) and one client bridge (AP3). However, the client bridge (AP3) is connecting to both AP1 and AP2 and using its link to base bridge (AP1) to forward traffic.

Resolution:

This is valid behavior. You see this when your mesh APs are close enough (in proximity) so the client bridge can see both the base bridges (AP1, AP2), in which case it forms two links, one each to AP1 and AP2. Since the link to AP1 is the shortest path in terms of number of hops, AP3 uses that link to forward traffic.

Mesh Deployment Issue 3 - Cannot select a WLAN name for a Client Bridge

You created a WLAN for mesh backhaul on an AP needed as a client bridge, but you don't get to select the WLAN name in the *Mesh Network Name* drop down menu. Why?

Resolution:

Check the WLAN configuration to ensure you have enabled the *Enable Client Bridge Backhaul* option.

Mesh Deployment Issue 4 - Do I need to map a WLAN to a radio when configuring mesh backhaul on a Client Bridge?

When creating a mesh backhaul WLAN on a client bridge only AP, do you need to map the WLAN on a radio?

Resolution:

No, a client bridge only AP behaves just like an MU! It scans for base bridges and forms connections to them. It doesn't need to beacon on that WLAN. Therefore, while creating a mesh backhaul WLAN on a client bridge only AP, just enable the *Enable Client Bridge Backhaul* option.

Mesh Deployment Issue 5 - Do I need to use secure beacons on a mesh backhaul supported WLAN?

Can I use secure beacons on the mesh backhaul supported WLAN?

Resolution:

Yes, you can enable a secure beacon on a mesh backhaul supported WLAN. In fact, it is a Extreme Networks recommended practice.

Mesh Deployment Issue 6 - Is my mesh topology complete?

How can I determine if all my mesh APs are connected and the mesh topology is complete?

Resolution:

Each mesh AP has a *Known AP Table* (available in the applet, CLI and SNMP). All APs (whether they are supporting mesh or not) periodically exchange ID messages notifying their presence to one another. Review the Known AP Table on any mesh supported AP to determine if you have all required APs connected to the mesh topology.

Mesh Deployment Issue 7 - Can MUs roam within a mesh topology?

Can MUs connected to a mesh AP roam seemlessly among other MUs and wired Access Points?

Resolution:

Yes, MUs on a mesh APs can roam seemlessly throughout the mesh network as well as with non-mesh Access Points on the wired network.

Mesh Deployment Issue 8 - Can I mesh between an AP4700 and an AP3500?

Can I mesh between these models?

Resolution:

Yes, the Access Points are fairly close from a software deployment standpoint. So it is a supported configuration for three models to exist in a single topology.

Mesh Deployment Issue 9 - Can I perform firmware/configuration file updates with DHCP options?

Can I use the AP's Automatic Firmware/Configuration update functionalities with DHCP Options on the AP for mesh nodes as well?

Resolution:

Yes, mesh nodes also support Automatic Firmware/Configuration updates using DHCP Options. Make sure you create DHCP reservations for each mesh node and add an appropriate configuration file to each one of them. If you don't, the base bridge configuration file could get applied on a client bridge or repeater and you will loose connectivity to that AP.

Mesh Deployment Issue 10 - Why do I lose connectivity when updating configurations?

When I make a configuration change and apply the changes on a client bridge or repeater, I momentarily loose connectivity to that AP, why?

Resolution:

That is expected behavior, when you make a configuration change on a mesh supported AP, it brings the radio driver down and then back up again. Consequently, the AP needs to re-establish its mesh connection after saving the configuration.

Mesh Deployment Issue 11 - Will an existing client bridge see a new base bridge or repeater?

If I add a new base bridge or repeater to an existing mesh topology, will my current client bridges see it and connect to it?

Resolution:

Yes, all client bridges perform periodic background scanning - both passively (by sniffing the air for beacons) and actively (by sending Probe Requests). Therefore, a client bridge automatically detects the presence of a new base bridge or repeater added to the mesh network topology and forms a seam less connection without affecting current operation.

Mesh Deployment Issue 12 - Can a mesh supported AP react to changing RF conditions?

If RF conditions change, will a mesh supported AP automatically detect and re-route traffic on its backup link or look for new links if all current links are exhausted?

Resolution:

Yes, all mesh nodes have built in dynamic link switching and auto-recovery mechanisms that ensure they adapt to changing RF conditions.

10 CHAPTER Adaptive AP

An adaptive AP (AAP) is an access point that can adopt like a thin AP in layer 2 or layer 3. The management of an AAP is conducted by the controller, once the access point connects to an Extreme Networks WM3000 series wireless controller and receives its AAP configuration. Refer to the following for Adaptive AP configuration activities supported by the access point user interface:

Adaptive AP Overview

An *adaptive AP* (AAP) is an Access Point that can adopt like an Altitude 4600 Series Access Point (L3). The management of an AAP is conducted by the controller, once the Access Point connects to a Extreme Networks controller and receives its AAP configuration.

An AAP provides:

- local 802.11 traffic termination
- local encryption/decryption
- local traffic bridging
- the tunneling of centralized traffic to the wireless controller

An AAP's controller connection can be secured using IP/UDP or IPSec depending on whether a secure WAN link from a remote site to the central site already exists.

The controller can be discovered using one of the following mechanisms:

- DHCP
- Controller *fully qualified domain name* (FQDN)
- Static IP addresses

The benefits of an AAP deployment include:

- *Centralized Configuration Management & Compliance*—Wireless configurations across distributed sites can be centrally managed by the wireless controller or cluster.

- *WAN Survivability*—Local WLAN services at a remote sites are unaffected in the case of a WAN outage.
- *Securely extend corporate WLAN's to stores for corporate visitors*—Small home or office deployments can utilize the feature set of a corporate WLAN from their remote location.
- *Maintain local WLAN's for in store applications*—WLANs created and supported locally can be concurrently supported with your existing infrastructure.

Where to Go From Here

Refer to the following for a further understanding of AAP operation:

- Adaptive AP Management on page 606
- Licensing on page 606
- Controller Discovery on page 607
- Securing a Configuration Channel Between Controller and AP on page 608
- Adaptive AP WLAN Topology on page 609
- Configuration Updates on page 609
- Securing Data Tunnels between the Controller and AAP on page 609
- Adaptive AP Controller Failure on page 609
- Remote Site Survivability (RSS) on page 610
- Adaptive Mesh Support on page 610

For an understanding of how AAP support should be configured for the Access Point and its connected controller, see "How the AP Receives its Adaptive Configuration" on page 612.

For an overview of how to configure both the Access Point and controller for basic AAP connectivity and operation, see "Establishing Basic Adaptive AP Connectivity" on page 614.

To configure the Access Point's controller discovery method and connection medium, see "Adaptive AP Setup" on page 85.

Adaptive AP Management

An AAP can be adopted, configured and managed like a thin Access Port from the wireless controller. Once an Access Point connects to a controller and receives its AAP configuration, its WLAN and radio configuration is similar to a thin Access Port. An AAP's radio mesh configuration can also be configured from the controller. However, non-wireless features (DHCP, NAT, Firewall etc.) cannot be configured from the controller and must be defined using the Access Point's resident interfaces before its conversion to an AAP.

Licensing

An AAP uses the same licensing scheme as a thin Access Port. This implies an existing license purchased with a controller can be used for an AAP deployment. Regardless of how many AAPs are deployed, you must ensure the license used by the controller supports the number of Access Points you intend to adopt.

Controller Discovery

For an Access Point to function as an AAP (regardless of mode), it needs to connect to a controller to receive its configuration. There are two methods of controller discovery:

- Auto Discovery Using DHCP on page 607
- Manual Adoption Configuration on page 608v

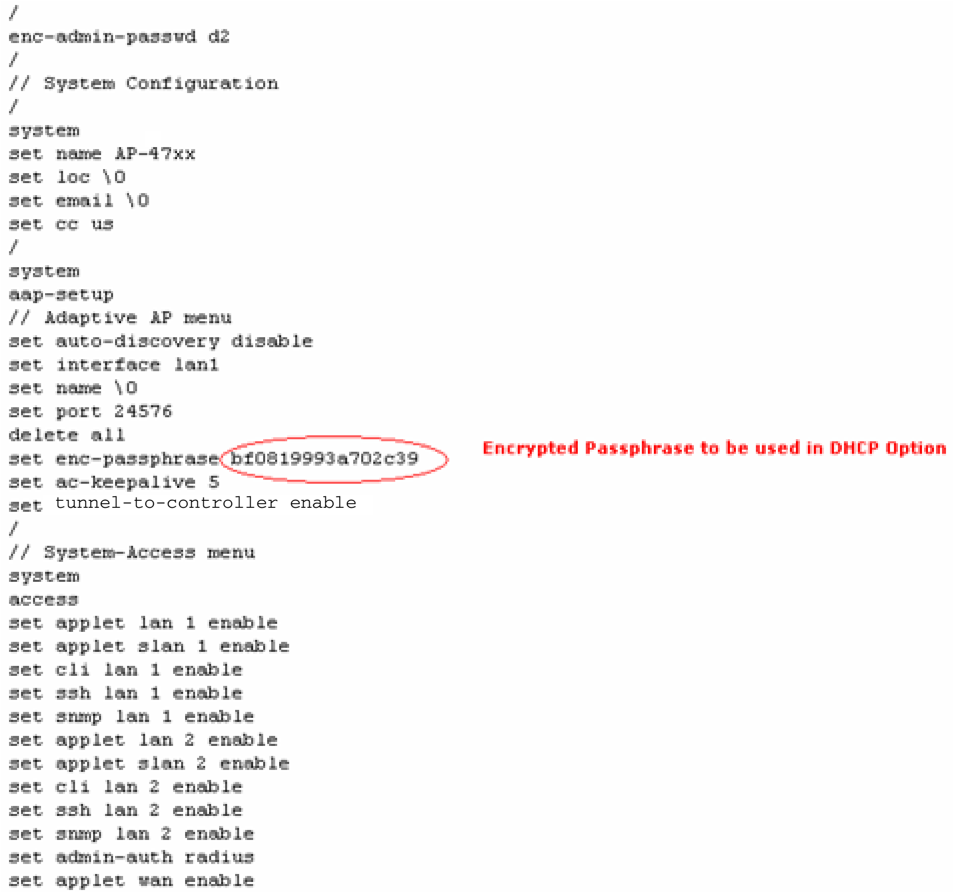
Auto Discovery Using DHCP

Extended Global Options 189, 190, 191, 192 can be used or Embedded Option 43 - Vendor Specific options can be embedded in Option 43 using the vendor class identifier: ExtremeAP.4700.

Table 1: Auto Discovery Using DHCP

	Code	**Data Type**
List of Controller IP addresses *(separate by comma, semi-colon, or space delimited)*	188	String
Controller FQDN	190	String
Access Point Encryption IPSec Passphrase (Hashed) **	191	String
Access Point controller discovery mode 1 = auto discovery enable 2 = auto discover enabled (using IPSec)	192	String

** The Access Point uses an encryption key to hash passphrases and security keys. To obtain the passphrase, configure an Access Point with the passphrase and export the configuration file.



```
/
enc-admin-passwd d2
/
// System Configuration
/
system
set name AP-47xx
set loc \0
set email \0
set cc us
/
system
aap-setup
// Adaptive AP menu
set auto-discovery disable
set interface lan1
set name \0
set port 24576
delete all
set enc-passphrase bf0819993a702c39
set ac-keepalive 5
set tunnel-to-controller enable
/
// System-Access menu
system
access
set applet lan 1 enable
set applet slan 1 enable
set cli lan 1 enable
set ssh lan 1 enable
set snmp lan 1 enable
set applet lan 2 enable
set applet slan 2 enable
set cli lan 2 enable
set ssh lan 2 enable
set snmp lan 2 enable
set admin-auth radius
set applet wan enable
```

Encrypted Passphrase to be used in DHCP Option

Manual Adoption Configuration

A manual controller adoption of an AAP can be conducted using:

- *Static FQDN*—A controller fully qualified domain name can be specified to perform a DNS lookup and controller discovery.
- *Static IP addresses*—Up to 12 controller IP addresses can be manually specified in an ordered list the AP can choose from. When providing a list, the AAP tries to adopt based on the order in which they are listed (from 1-12).

NOTE

An AAP can use its LAN or WAN Ethernet interface to adopt. The LAN is PoE and DHCP enabled by default.

The WAN has no PoE support and has a default static AP address of 10.1.1.1/8.

Securing a Configuration Channel Between Controller and AP

Once an Access Point obtains a list of available controllers, it begins connecting to each. The controller can be either on the LAN or WAN side of the Access Point to provide flexibility in the deployment of the network. If the controller is on the Access Point's LAN, ensure the LAN subnet is on a secure channel. The AP will connect to the controller and request a configuration.

Adaptive AP WLAN Topology

An AAP can be deployed in the following WLAN topologies:

- *Extended WLANs*—Extended WLANs are the centralized WLANs created on the controller.
- *Independent WLANs*—Independent WLANs are local to an AAP and can be configured from the controller. You must specify a WLAN as independent to stop traffic from being forwarded to the controller. Independent WLANs behave like WLANs on a standalone Access Point.
- *Both*—Extended and independent WLANs are configured from the controller and operate simultaneously.

NOTE

For a review of some important considerations impacting the use of extended and independent WLANs within an AAP deployment, see "Adaptive AP Deployment Considerations" on page 619.

Configuration Updates

An AAP receives its configuration from the controller initially as part of its adoption sequence. Subsequent configuration changes on the controller are reflected on an AAP when applicable.

An AAP applies the configuration changes it receives from the controller after 30 seconds from the last received controller configuration message. When the configuration is applied on the AAP, the radios shutdown and re-initialize (this process takes less than 2 seconds) forcing associated MUs to be deauthenticated. MUs are quickly able to associate.

Securing Data Tunnels between the Controller and AAP

If a secure link (site-to-site VPN) from a remote site to the central location already exists, the AAP does not require IPSec be configured for adoption.

For sites with no secure link to the central location, an AAP can be configured to use an IPSec tunnel (with AES 256 encryption) for adoption. The tunnel configuration is automatic on the AAP side and requires no manual VPN policy be configured. On the controller side, configuration updates are required to adopt the AAP using an IPSec tunnel.

To review a sample AAP configuration, see "Sample Controller Configuration File for IPSec and Independent WLAN" on page 620.

Adaptive AP Controller Failure

In the event of a controller failure, an AAP's independent WLAN continues to operate without disruption. The AAP attempts to connect to other controllers (if available) in background. Extended WLANs are disabled once controller adoption is lost. When a new controller is discovered and a connection is secured, an extended WLAN can be enabled.

If a new controller is located, the AAP synchronizes its configuration with the located controller once adopted. If *Remote Site Survivability* (RSS) is disabled, the independent WLAN is also disabled in the event of a controller failure.

Remote Site Survivability (RSS)

RSS can be used to turn off RF activity on an AAP if it loses adoption (connection) to the controller.

RSS State	Independent WLANs	Extended WLANs
RSS Enabled	WLAN continues beaconing	WLAN continues beaconing but AP does allow clients to associate on that WLAN
RSS Disabled	WLAN stops beaconing	WLAN stops beaconing

NOTE

For a dependant AAP, independent WLANs continue to beacon for three days in the absence of a controller.

Adaptive Mesh Support

An AAP can extend existing mesh functionality to a controller managed network. All mesh APs are configured and managed through the wireless controller. APs without a wired connection form a mesh backhaul to a repeater or a wired mesh node and then get adopted to the controller. Mesh nodes with existing wired access get adopted to the controller like a wired AAP.

Mesh AAPs apply configuration changes 300 seconds after the last received controller configuration message. When the configuration is applied on the Mesh AAP, the radios shutdown and re-initialize (this process takes less than 2 seconds), forcing associated MUs to be deauthenticated and the Mesh link will go down. MUs are able to quickly associate, but the Mesh link will need to be re-established before MUs can pass traffic. This typically takes about 90 to 180 seconds depending on the size of the mesh topology.

NOTE

When mesh is used with AAPs, the “ap-timeout” value needs to be set to a higher value (for example, 180 seconds) so Mesh AAPs remain adopted to the controller during the period when the configuration is applied and mesh links are re-established.

For an overview of mesh networking and how to configure an Access Point to support mesh, see “Configuring Mesh Networking” on page 577.

Supported Adaptive AP Topologies

For this version of the Access Point firmware, the following AAP topologies are supported:

- Extended WLANs Only on page 611
- Independent WLANs Only on page 611

- Extended WLANs with Independent WLANs on page 612
- Extended WLAN with Mesh Networking on page 612

Topology Deployment Considerations

When reviewing the AAP topologies describes in the section, be cognizant of the following considerations to optimize the effectiveness of the deployment:

- An AAP firmware upgrade will not be performed at the time of adoption from the wireless controller. Instead, the firmware is upgraded using the firmware update procedure (manually or using the DHCP Auto Update feature).
- An AAP can use its LAN1 interface or WAN interface for adoption. The default gateway interface is set to LAN1. If the WAN Interface is used, explicitly configure WAN as the default gateway interface.
- Extreme Networks recommends using the LAN1 interface for adoption in multi-cell deployments.
- If you have multiple independent WLANs mapped to different VLANs, the AAP's LAN1 interface requires trunking be enabled with the correct management and native VLAN IDs configured. Additionally, the AAP needs to be connected to a 802.1q trunk port on the wired controller.
- Be aware IPSec Mode supports NAT Traversal (NAT-T).

Extended WLANs Only

An extended WLAN configuration forces all MU traffic through the controller. No wireless traffic is locally bridged by the AAP.

Each extended WLAN is mapped to the Access Point's virtual LAN2 subnet. By default, the Access Point's LAN2 is not enabled and the default configuration is set to static with IP addresses defined as all zeros. If the extended VLAN option is configured on the controller, the following configuration updates are made automatically:

- The AAP’s LAN2 subnet becomes enabled
- All extended VLANs are mapped to LAN2.

NOTE

MUs on the same WLAN associated to the AAP can communicate locally at the AP Level without going through the controller. If this scenario is undesirable, the Access Point's MU-to-MU disallow option should be enabled. To enable the Access Point’s MU-to-MU disallow option, see “Creating/Editing Individual WLANs” on page 148.

Independent WLANs Only

An independent WLAN configuration forces all MU traffic be bridged locally by the AAP. No wireless traffic is tunneled back to the controller. Each extended WLAN is mapped to the Access Point's LAN1 interface. The only traffic between the controller and the AAP are control messages (for example, heartbeats, statistics and configuration updates).

Extended WLANs with Independent WLANs

An AAP can have both extended WLANs and independent WLANs operating in conjunction. When used together, MU traffic from extended WLANs go back to the controller and traffic from independent WLANs is bridged locally by the AP.

All local WLANs are mapped to LAN1, and all extended WLANs are mapped to LAN2.

Extended WLAN with Mesh Networking

Mesh networking is an extension of the existing wired network. There is no special configuration required, with the exceptions of setting the mesh and using it within one of the two extended VLAN configurations and defining an Access Point radio as a preferred base bridge.

NOTE

The mesh backhaul WLAN must be an independent WLAN mapped to LAN1. The controller enforces the WLAN be defined as an independent WLAN by automatically setting the WLAN to independent when backhaul is selected. The AP ensures the backhaul WLAN be put on LAN1.

How the AP Receives its Adaptive Configuration

An AAP does not require a separate “local” or “running” configuration. Once enabled as an AAP, the AP obtains its configuration from the controller. If the AP’s WAN link fails, it continues to operate using the last valid configuration until its link is re-established and a new configuration is pushed down from the controller. There is no separate file-based configuration stored on the controller.

Only WLAN, VLAN extension and radio configuration items are defined for the AAP by its connected controller. None of the other Access Point configuration items (RADIUS, DHCP, NAT, Firewall etc.) are configurable from the connected controller.

After the AP downloads a configuration file from the controller, it obtains the version number of the image it should be running. The controller does not have the capacity to hold the Access Point’s firmware image and configuration. The Access Point image must be downloaded using a means outside the controller. If there is still an image version mismatch between what the controller expects and what the AAP is running, the controller will deny adoption.

Adaptive AP Prerequisites

Converting an Access Point into an AAP requires:

- A version 2.0 or higher firmware running on the Access Point.
- A Summit WM3400, Summit WM3600 or Summit WM3700 controller.
- The appropriate controller licenses providing AAP functionality on the controller.
- The correct password to authenticate and connect the adaptive to the controller.

Configuring the Adaptive AP for Adoption by the Controller

1 An AAP needs to find and connect to the controller. To ensure this connection:

- Configure the controller's IP address on the AAP
- Provide the controller IP address using DHCP option 189 on a DHCP server. The IP address is a comma delimited string of IP addresses. For example "157.235.94.91, 10.10.10.19". There can be a maximum of 12 IP addresses.
- Configure the controller's FQDN on the AAP. The AAP can use this to resolve the IP address of the controller.

2 Use the controller's secret password on the AAP for the controller to authenticate it.

For additional information on defining the connection medium used by the Access Point t to receive an AAP configuration, see "Adaptive AP Setup" on page 85.

To avoid a lengthy broken connection with the controller, Extreme Networks recommends generating an SNMP trap when the AAP loses adoption with the controller.

NOTE

For additional information (in greater detail) on the AP configuration activities described above, see "Adaptive AP Configuration" on page 614.

Configuring the Controller for Adaptive AP Adoption

The tasks described below are configured on an Extreme Networks controller. For information on configuring the controller for AAP support, see http://www.extremenetworks.com/go/documentation.

To adopt an AAP on a controller:

1 Ensure enough licenses are available on the controller to adopt the required number of AAPs.

2 As soon as the AAP displays in the adopted list:

Adjust each AAP's radio configuration as required. This includes WLAN-radio mappings and radio parameters. WLAN-VLAN mappings and WLAN parameters are global and cannot be defined on a per radio basis. WLANs can be assigned to a radio. Optionally, configure WLANs as independent and assign to AAPs as needed.

3 Configure each VPN tunnel with the VLANs to be extended to it.

If you do not attach the target VLAN, no data will be forwarded to the AAP, only control traffic required to adopt and configure the AP.

NOTE

For additional information (in greater detail) on the controller configuration activities described above, see "Controller Configuration" on page 616.

Establishing Basic Adaptive AP Connectivity

This section defines the activities required to configure basic AAP connectivity with a Summit WM3400, Summit WM3600 or Summit WM3700 controller. In establishing a basic AAP connection, both the Access Point and controller require modifications to their respective default configurations. For more information, see:

- Adaptive AP Configuration on page 614
- Controller Configuration on page 616

NOTE

Refer to *"Adaptive AP Deployment Considerations" on page 619* for usage and deployment caveats that should be considered before defining the AAP configuration. Refer to *"Sample Controller Configuration File for IPSec and Independent WLAN" on page 620* if planning to deploy an AAP configuration using IPSec VPN and an extended WLAN.

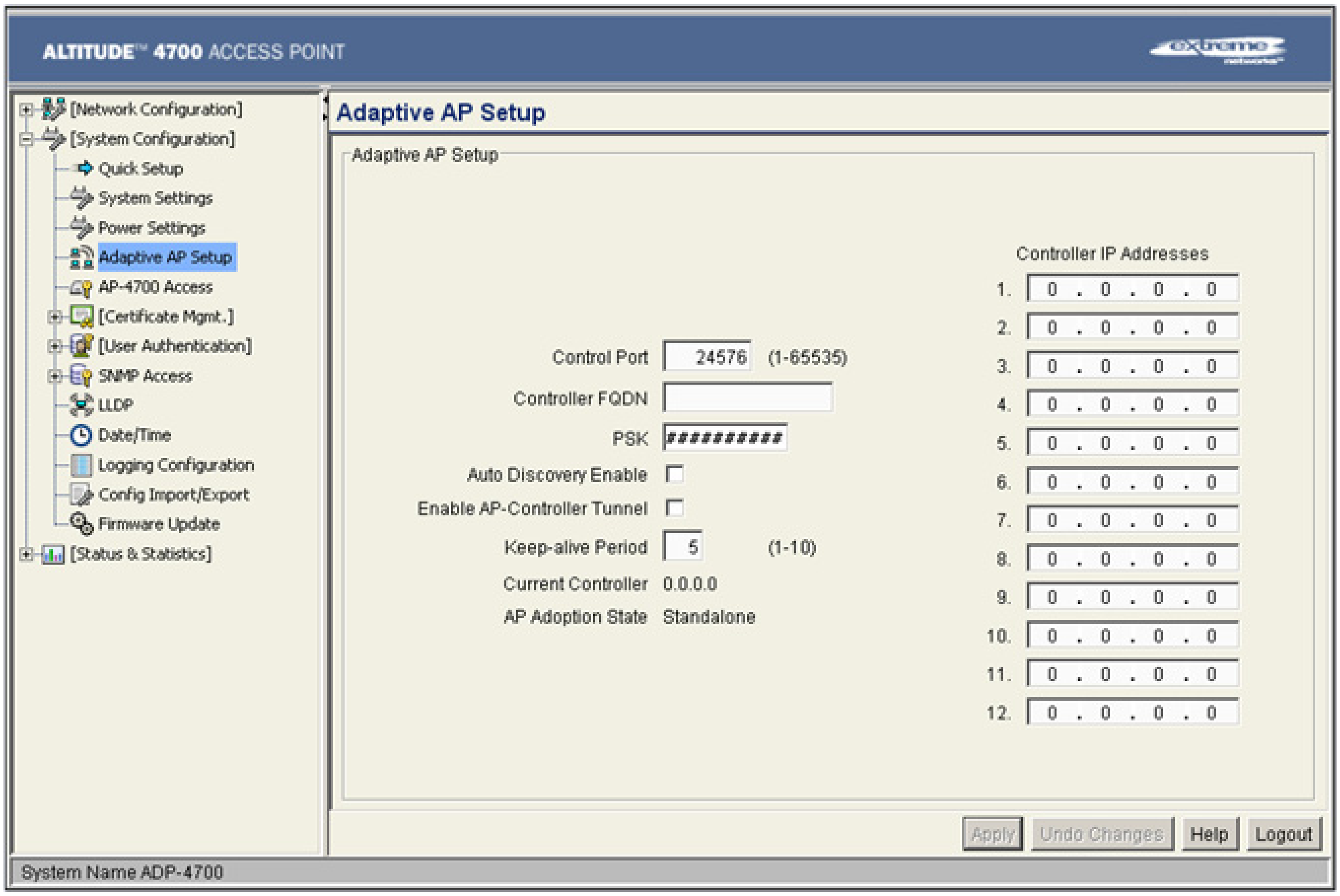
Adaptive AP Configuration

An AAP can be manually adopted by the controller, adopted using a configuration file (consisting of the adaptive parameters) pushed to the Access Point or adopted using DHCP options. Each of these adoption techniques is described in the sections that follow.

Adopting an Adaptive AP Manually

To manually enable the Access Point’s controller discovery method and connection medium required for adoption:

1 Select *System Configuration* > *Adaptive AP Setup* from the Access Point’s menu tree.



Adaptive AP Setup

Adaptive AP Setup

Control Port 24576 (1-65535)

Controller FQDN

PSK ###########

Auto Discovery Enable □

Enable AP-Controller Tunnel □

Keep-alive Period 5 (1-10)

Current Controller 0.0.0.0

AP Adoption State Standalone

Controller IP Addresses

1. 0 . 0 . 0 . 0
2. 0 . 0 . 0 . 0
3. 0 . 0 . 0 . 0
4. 0 . 0 . 0 . 0
5. 0 . 0 . 0 . 0
6. 0 . 0 . 0 . 0
7. 0 . 0 . 0 . 0
8. 0 . 0 . 0 . 0
9. 0 . 0 . 0 . 0
10. 0 . 0 . 0 . 0
11. 0 . 0 . 0 . 0
12. 0 . 0 . 0 . 0

System Name ADP-4700

2 Select the *Auto Discovery Enable* checkbox.

Enabling auto discovery will allow the AAP to be detected by a controller once its connectivity medium has been configured (by completing steps 3-6)

3 Enter up to 12 *Controller IP Addresses* constituting the target controllers available for AAP connection.

The AAP will begin establishing a connection with the first addresses in the list. If unsuccessful, the AP will continue down the list (in order) until a connection is established.

4 If a numerical IP address is unknown, but you know a controller’s *fully qualified domain name* (FQDN), enter the name as the *Controller FQDN* value.

5 Select the *Enable AP-Controller Tunnel* option to allow AAP configuration data to reach a controller using a secure VPN tunnel.

6 If using IPSec as the tunnel resource, enter the IPSec *Passkey* to ensure IPSec connectivity.

7 Click *Apply* to save the changes to the AAP setup.

NOTE

The manual AAP adoption described above can also be conducted using the Access Point's CLI interface using the *admin(system.aapsetup)> command.*

Adopting an Adaptive AP Using a Configuration File

To adopt an AAP using a configuration file:

1 Refer to "Adopting an Adaptive AP Manually" and define the AAP controller connection parameters.

2 Export the AAP's configuration to a secure location.

Either import the configuration manually to other APs or the same AP later (if you elect to default its configuration). Use DHCP option 186 and 187 to force a download of the configuration file during startup (when it receives a DHCP offer).

For instruction on how to use the Access Point's configuration import/export functionality, see "Importing/Exporting Configurations" on page 114.

For information on updating the Access Point's firmware, see "Updating Device Firmware" on page 118.

Adopting an Adaptive AP Using DHCP Options

An AAP can be adopted to a wireless controller by providing the following options in the DHCP Offer:

Option	Data Type	Value
189	String	<Controller IP Address or Range of IP addresses separated by [, ; <space>]>
190	String	<Fully qualified Domain Name for the Wireless Controller>
191	String	<Hashed IPSec Passkey - configure on 1 AP and export to get hashed key>
192	String	<Value of "1" denotes Non-IPSec Mode and "2" denotes IPSec Mode>

NOTE

Options 189 and 192 are mandatory to trigger adoption using DHCP options. Unlike an Altitude 4600, option 189 alone won't work. These options can be embedded in Vendor Specific Option 43 and sent in the DHCP Offer.

Controller Configuration

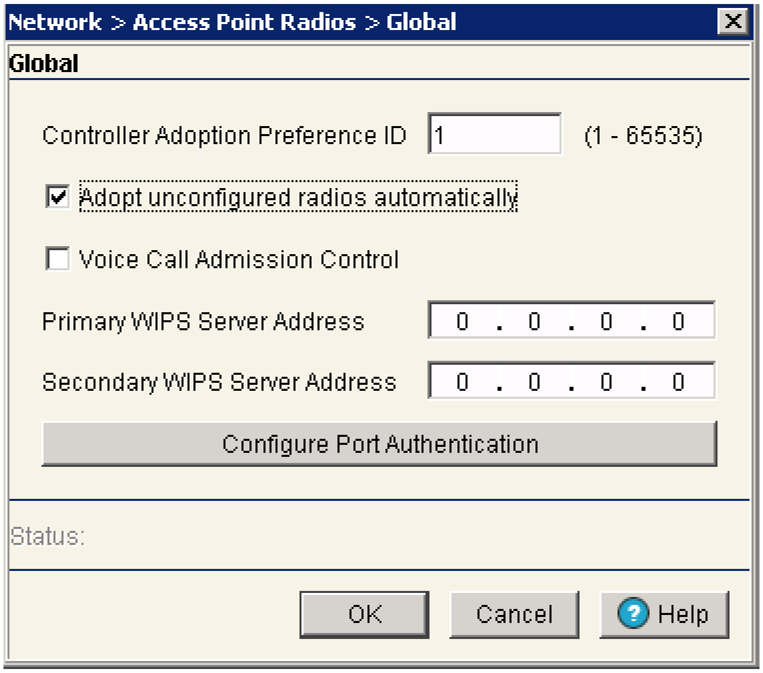
A Summit WM3400, Summit WM3600 and Summit WM3700 controller require an explicit adaptive configuration to adopt an Access Point (if IPSec is not being used for adoption). The same licenses currently used for Altitude 4600 adoption can be used for an AAP.

Disable the controller's *Adopt unconfigured radios automatically* option and manually add AAPs requiring adoption, or leave as default. In default mode, any AAP adoption request is honored until the current controller license limit is reached.

To disable automatic adoption on the controller:

1 Select *Network* > *Access Port Radios* from the controller main menu tree.

2 Select the *Configuration* tab (should be displayed be default) and click the *Global Settings* button.



Network > Access Point Radios > Global

Global

Controller Adoption Preference ID: 1 (1 - 65535)

☑ Adopt unconfigured radios automatically

□ Voice Call Admission Control

Primary WIPS Server Address: 0 . 0 . 0 . 0

Secondary WIPS Server Address: 0 . 0 . 0 . 0

3 Ensure the *Adopt unconfigured radios automatically* option is NOT selected.

When disabled, there is no automatic adoption of non-configured radios on the network. Additionally, default radio settings will NOT be applied to Access Ports when automatically adopted.

NOTE

For IPSec deployments, refer to "Sample Controller Configuration File for IPSec and Independent WLAN" on page 620 and take note of the CLI commands in red and associated comments in green.

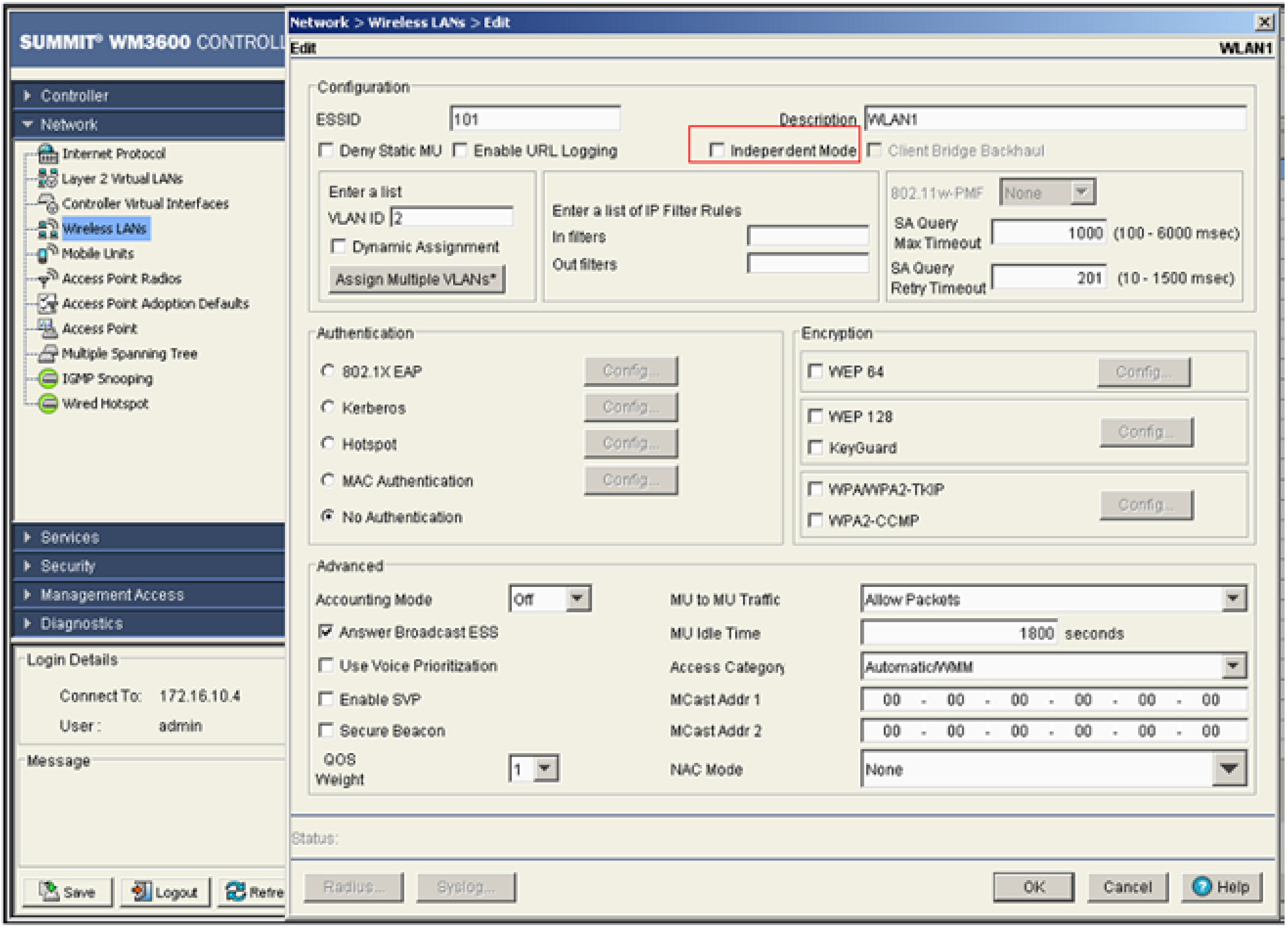
Any WLAN configured on the controller becomes an extended WLAN by default for an AAP.

4 Select *Network* > *Wireless LANs* from the controller main menu tree.

5 Select the target WLAN you would like to use for AAP support from those displayed and click the *Edit* button.

6 Select the *Independent Mode (AAP Only)* checkbox.

7 Selecting the checkbox designates the WLAN as independent and prevents traffic from being forwarded to the controller. Independent WLANs behave like WLANs as used on a a standalone Access Point. Leave this option unselected (as is by default) to keep this WLAN an extended WLAN (a typical centralized WLAN created on the controller).



WLAN1

ESSID 101

Description WLAN1

☐ Deny Static MU ☐ Enable URL Logging ☐ Independent Mode ☐ Client Bridge Backhaul

VLAN ID 2

☐ Dynamic Assignment

802.11w-PMF None

SA Query Max Timeout 1000 (100 - 6000 msec)

SA Query Retry Timeout 201 (10 - 1500 msec)

Authentication

○ 802.1X EAP
○ Kerberos
○ Hotspot
○ MAC Authentication
● No Authentication

Encryption

☐ WEP 64
☐ WEP 128
☐ KeyGuard
☐ WPA/WPA2-TKIP
☐ WPA2-CCMP

Advanced

Accounting Mode Off
☑ Answer Broadcast ESS
☐ Use Voice Prioritization
☐ Enable SVP
☐ Secure Beacon
QOS Weight 1

MU to MU Traffic Allow Packets
MU Idle Time 1800 seconds
Access Category Automatic/WMM
MCast Addr 1 00 - 00 - 00 - 00 - 00 - 00
MCast Addr 2 00 - 00 - 00 - 00 - 00 - 00
NAC Mode None

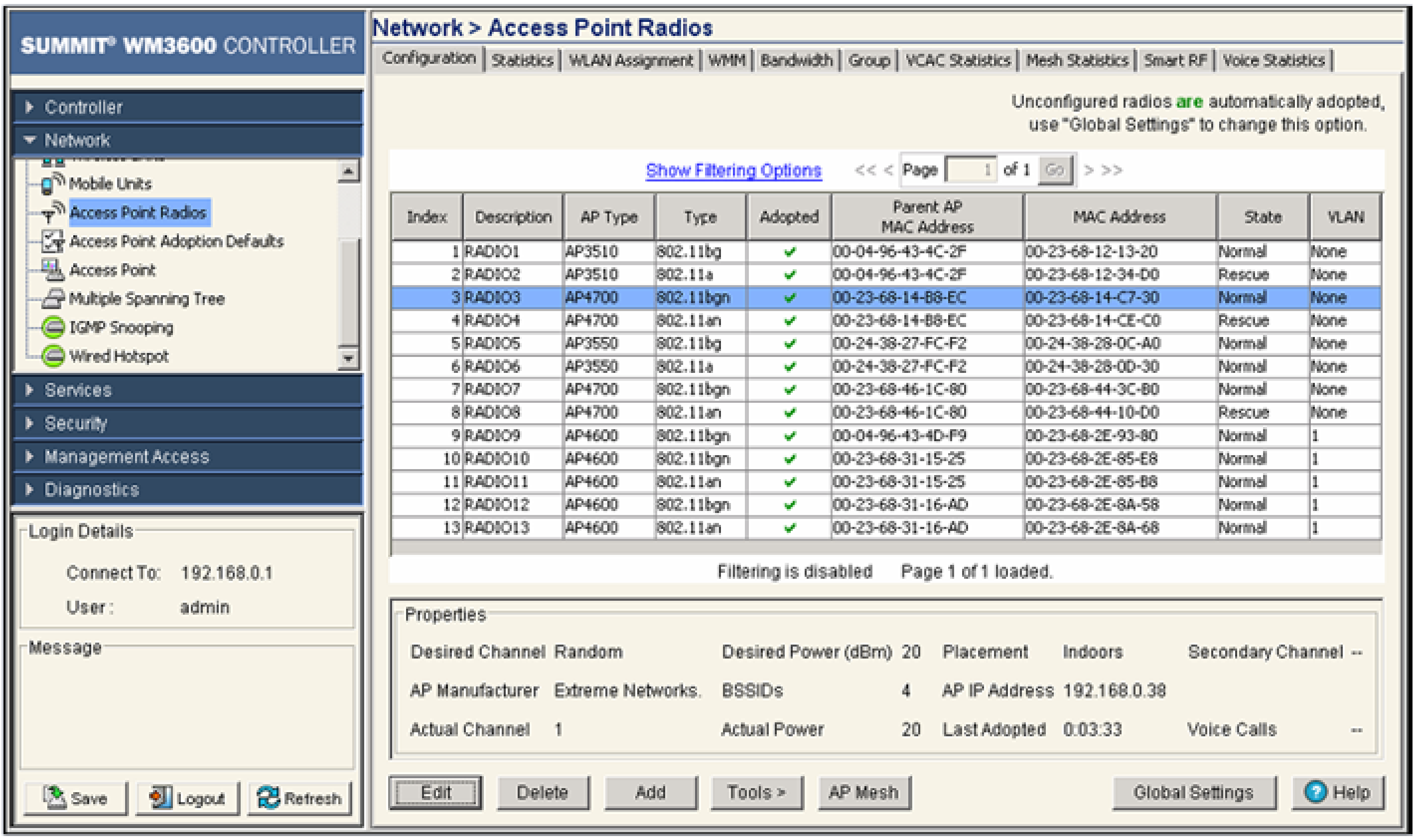
Login Details

Connect To: 172.16.10.4
User : admin

NOTE

Additionally, a WLAN can be defined as independent using the "*wlan <index> independent*" command from the config-wireless context.

Once an AAP is adopted by the controller, it displays within the controller *Access Port Radios* screen (under the Network parent menu item) as an Access Point within the *AP Type* column.



Network > Access Point Radios

Login Details

Connect To: 192.168.0.1

User : admin

Message

Unconfigured radios are automatically adopted, use "Global Settings" to change this option.

Index	Description	AP Type	Type	Adopted	Parent AP MAC Address	MAC Address	State	VLAN
1	RADIO1	AP3510	802.11bg	✓	00-04-96-43-4C-2F	00-23-68-12-13-20	Normal	None
2	RADIO2	AP3510	802.11a	✓	00-04-96-43-4C-2F	00-23-68-12-34-D0	Rescue	None
3	RADIO3	AP4700	802.11bgn	✓	00-23-68-14-B8-EC	00-23-68-14-C7-30	Normal	None
4	RADIO4	AP4700	802.11an	✓	00-23-68-14-B8-EC	00-23-68-14-CE-C0	Rescue	None
5	RADIO5	AP3550	802.11bg	✓	00-24-38-27-FC-F2	00-24-38-28-0C-A0	Normal	None
6	RADIO6	AP3550	802.11a	✓	00-24-38-27-FC-F2	00-24-38-28-0D-30	Normal	None
7	RADIO7	AP4700	802.11bgn	✓	00-23-68-46-1C-80	00-23-68-44-3C-80	Normal	None
8	RADIO8	AP4700	802.11an	✓	00-23-68-46-1C-80	00-23-68-44-10-D0	Rescue	None
9	RADIO9	AP4600	802.11bgn	✓	00-04-96-43-4D-F9	00-23-68-2E-93-80	Normal	1
10	RADIO10	AP4600	802.11bgn	✓	00-23-68-31-15-25	00-23-68-2E-85-E8	Normal	1
11	RADIO11	AP4600	802.11an	✓	00-23-68-31-15-25	00-23-68-2E-85-B8	Normal	1
12	RADIO12	AP4600	802.11bgn	✓	00-23-68-31-16-AD	00-23-68-2E-8A-58	Normal	1
13	RADIO13	AP4600	802.11an	✓	00-23-68-31-16-AD	00-23-68-2E-8A-68	Normal	1

Filtering is disabled   Page 1 of 1 loaded.

Properties

Desired Channel	Random	Desired Power (dBm)	20	Placement	Indoors	Secondary Channel	--
AP Manufacturer	Extreme Networks.	BSSIDs	4	AP IP Address	192.168.0.38		
Actual Channel	1	Actual Power	20	Last Adopted	0:03:33	Voice Calls	--

Adaptive AP Deployment Considerations

Before deploying your controller/AAP configuration, refer to the following usage caveats to optimize its effectiveness:

- Extended WLANs are mapped to the AP's LAN2 interface and all independent WLANs are mapped to the AP's LAN1 Interface.
- If deploying multiple independent WLANs mapped to different VLANs, ensure the AP's LAN1 interface is connected to a trunk port on the L2/L3 controller and appropriate management and native VLANs are configured.
- The WLAN used for mesh backhaul must always be an independent WLAN.
- The controller configures an AAP. If manually changing wireless settings on the AP, they are not updated on the controller. It's a one way configuration, from the controller to the AP.
- An AAP always requires a router between the AP and the controller.
- An AAP can be used behind a NAT.
- An AAP uses UDP port 24576 for control frames and UDP port 24577 for data frames.
- Multiple VLANs per WLAN, L3 mobility, dynamic VLAN assignment, NAC, self healing, rogue AP, MU locationing, hotspot on extended WLAN are some of the important wireless features not supported in an AAP supported deployment.

Sample Controller Configuration File for IPSec and Independent WLAN

The following constitutes a sample Summit WM3700 wireless LAN controller configuration file supporting an AAP IPSec with Independent WLAN configuration. Please note new AAP specific CLI commands in red and relevant comments in blue.

NOTE

In addition to the sample configuration below, a WMM policy should be enabled and configured for the Access Point in AAP mode.

The sample output is as follows:

```
!
! configuration of WM3700 WM3700-1
!
version 1.0
!
!
aaa authentication login default none
service prompt crash-info
!
hostname WM3700-1
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
To configure the ACL to be used in the CRYPTO MAP
!
ip access-list extended AAP-ACL permit ip host 10.10.10.250 any rule-precedence 20
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst config
name My Name
!
country-code us
logging buffered 4
logging console 7
logging host 157.235.92.97
logging syslog 7
snmp-server sysname WM3700-1
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5 0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpmanager v3 encrypted auth md5 0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpoperator v3 encrypted auth md5 0x49c451c7c6893ffcede0491bbd0a12c4
!
To configure the passkey for a Remote VPN Peer - 255.255.255.255 denotes all AAPs.
12345678 is the default passkey. If you change on the AAP, change here as well.
!
crypto isakmp key 0 12345678 address 255.255.255.255
```

```
!
ip http server
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip ssh
no service pm sys-restart
timezone America/Los_Angeles
license AP
xyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxx
yxyxyx
!
wireless
no adopt-unconf-radio enable
manual-wlan-mapping enable
wlan 1 enable
wlan 1 ssid qs5-ccmp
wlan 1 vlan 200
wlan 1 encryption-type ccmp
wlan 1 dot11i phrase 0 admin123
wlan 2 enable
wlan 2 ssid qs5-tkip
wlan 2 vlan 210
wlan 2 encryption-type tkip
wlan 2 dot11i phrase 0 admin123
wlan 3 enable
wlan 3 ssid qs5-wep128
wlan 3 vlan 220
wlan 3 encryption-type wep128
wlan 4 enable
wlan 4 ssid qs5-open
wlan 4 vlan 230
wlan 5 enable
wlan 5 ssid Mesh
wlan 5 vlan 111
wlan 5 encryption-type ccmp
wlan 5 dot11i phrase 0 admin123
!
To configure a WLAN as an independent WLAN
!
wlan 5 independent
wlan 5 client-bridge-backhaul enable
wlan 6 enable
wlan 6 ssid test-mesh
wlan 6 vlan 250
radio add 1 00-15-70-00-79-30 11bg aap4700
radio 1 bss 1 3
radio 1 bss 2 4
radio 1 bss 3 2
radio 1 channel-power indoor 11 8
radio 1 rss enable
radio add 2 00-15-70-00-79-30 11a aap4700
radio 2 bss 1 5
radio 2 bss 2 1
radio 2 bss 3 2
radio 2 channel-power indoor 48 8
radio 2 rss enable
radio 2 base-bridge max-clients 12
radio 2 base-bridge enable
radio add 3 00-15-70-00-79-12 11bg aap4700
radio 3 bss 1 3
radio 3 bss 2 4
radio 3 bss 3 2
radio 3 channel-power indoor 6 8
radio 3 rss enable
radio add 4 00-15-70-00-79-12 11a aap4700
radio 4 bss 1 5
radio 4 bss 2 6
radio 4 channel-power indoor 48 4
radio 4 rss enable
radio 4 client-bridge bridge-select-mode auto
radio 4 client-bridge ssid Mesh
radio 4 client-bridge mesh-timeout 0
radio 4 client-bridge enable
radio default-11a rss enable
radio default-11bg rss enable
radio default-11b rss enable
no ap-ip default-ap controller-ip
!
radius-server local
!
To create an IPSEC Transform Set
!
crypto ipsec transform-set AAP-TFSET esp-aes-256 esp-sha-hmac mode tunnel
!
To create a Crypto Map, add a remote peer, set the mode, add a ACL rule to match and
transform and set to the Crypto Map
!
crypto map AAP-CRYPTOMAP 10 ipsec-isakmp
set peer 255.255.255.255
set mode aggressive
match address AAP-ACL
set transform-set AAP-TFSET
!
interface ge1
controllerport mode trunk
controllerport trunk native vlan 1
controllerport trunk allowed vlan none
controllerport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
controllerport trunk allowed vlan add 180,190,200,210,220,230,240,250,
static-channel-group 1
!
interface ge2
controllerport access vlan 1
!
interface ge3
controllerport mode trunk
controllerport trunk native vlan 1
controllerport trunk allowed vlan none
controllerport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
controllerport trunk allowed vlan add 180,190,200,210,220,230,240,250,
static-channel-group 1
!
```

```
interface ge4
controllerport access vlan 1
!
interface me1
ip address dhcp
!
interface sa1
controllerport mode trunk
controllerport trunk native vlan 1
controllerport trunk allowed vlan none
controllerport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
controllerport trunk allowed vlan add 180,190,200,210,220,230,240,250,
!
!
!
!
interface vlan1
ip address dhcp
!
To attach a Crypto Map to a VLAN Interface
!
crypto map AAP-CRYPTOMAP
!
sole
!
ip route 157.235.0.0/16 157.235.92.2
ip route 172.0.0.0/8 157.235.92.2
!
ntp server 10.10.10.100 prefer version 3
line con 0
line vty 0 24
!
end
```

A

APPENDIX

Technical Specifications

This appendix section provides technical specifications for the following:

- Physical Characteristics on page 625
- Electrical Characteristics on page 626
- Radio Characteristics on page 626
- Country Codes on page 627

Physical Characteristics

This section describes the physical characteristics of the Altitude 4700 Series Access Points:

- Altitude 4710 and Altitude 4750 Physical Characteristics on page 625

Altitude 4710 and Altitude 4750 Physical Characteristics

An Altitude 4710 and Altitude 4750 Access Point has the following physical characteristics:

Table 2: Physical Characteristics

Dimensions	5.50 in. Depth x 7.88 in. Width x 1.38 in. Height 14 cm Depth x 20.32 cm Width x 3.5 cm Height
Housing	Metal, plenum-rated housing (UL2043)
Weight	2.7 lbs
Operating Temperature	-4°F to 122°F/-20°C to 50°C
Storage Temperature	-40°F to 158°F/-40°C to 70°C
Altitude	8000 ft./2438 m @ 82°F/28°C (Operating) 15000 ft./4572 m @ 53°F/12°C (Storage)
Humidity	5 to 95% RH non-condensing
Electrostatic Discharge	15kV air, 8kV contact

Electrical Characteristics

The Altitude 4700 Series Access Points have the following electrical characteristics:

Table 3: Electrical Characteristics

Operating Voltage	38-54V DC
Operating Current	Not to exceed 600mA @ 48VDC

Radio Characteristics

This section describes the radio characteristics of the Altitude 4700 Series Access Points:

- Altitude 4710 and Altitude 4750 Radio Characteristics on page 626

Altitude 4710 and Altitude 4750 Radio Characteristics

An Altitude 4710 and Altitude 4750 has the following radio characteristics:

Table 4: Radio Characteristics

Operating Channels	All channels from 4920 MHz to 5825 MHz except channel 52–64 Channels 1-13 (EU), Channels 1-11 (US/Canada) Channel 14 (2484 MHz) Japan only Actual operating frequencies depend on regulatory
Data Rates Supported	802.11g: 1,2,5.5,11,6,9,12,18,24,36,48, and 54Mbps 802.11a: 6,9,12,18,24,36,48, and 54Mbps 802.11n: MCS 0-15 up to 300Mbps
Wireless Medium	*Direct Sequence Spread Spectrum* (DSSS), *Orthogonal Frequency Division Multiplexing* (OFDM) *Spatial multiplexing* (MIMO)
Network Standards	802.11a, 802.11b, 802.11g, 802.3, 802.11n (Draft 2.0)
Maximum Available Transmit Power	Maximum available conducted transmit power per chain: 2.4Ghz: + 23 dBm Maximum available conducted transmit power all chains: 2.4GHz: + 27.7 dBm Maximum available conducted transmit power per chain: 5.2Ghz: + 20 dBm Maximum available conducted transmit power all chains: 5.2GHz: + 24.7 dBm
Transmit Power Adjustment	1 dB increments
Antenna Configuration	2x3 or 3x3

Country Codes

The following list of countries and their country codes is useful when using the Access Point configuration file, CLI or the MIB to configure the Access Point:

Table 5: Country Codes

Country	Code
Algeria	DZ
Anguilla	AI
Argentina	AR
Australia	AU
Austria	AT
Bahamas	BS
Bahrain	BH
Barbados	BB
Belarus	BY
Belgium	BE
Bermuda	BM
Bolivia	BO
Botswana	BW
Botznia-Herzegovina	BA
Brazil	BR
Bulgaria	BG
Canada	CA
Chile	CL
China	CN
Christmas Islands	CX
Colombia	CO
Costa Rica	CR
Croatia	HR
Cypress	CY
Czech Rep.	CZ
Denmark	DK
Dominican Republic	DO
Ecuador	EC
Egypt	EG
El Salvador	SV
Estonia	EE
Falkland Islands	FK
Finland	FI
France	FR
French Guiana	GF
Germany	DE

Table 5: Country Codes (Continued)

Country	Code
Greece	GR
Guadeloupe	GP
Guatemala	GT
Guyana	GY
Haiti	HT
Honduras	HN
Hong Kong	HK
Hungary	HU
Iceland	IS
India	IN
Indonesia	ID
Ireland	IE
Italy	IT
Jamaica	JM
Japan	JP
Jordan	JO
Kazakhstan	KZ
Kenya	KE
Kuwait	KW
Latvia	LV
Lebanon	LB
Liechtenstein	LI
Lithuania	LT
Luxembourg	LU
Macau	MO
Macedonia	MK
Malaysia	MY
Malta	MT
Martinique	MQ
Mexico	MX
Moldova	MD
Montenegro	ME
Morocco	MA
Nambia	NA
Netherlands	NL
Netherlands Antilles	AN
New Zealand	NZ
Nicaragua	NI
Nigeria	NG
Niue Island	NU
Norfolk Island	NF

Table 5: Country Codes (Continued)

Country	Code
Norway	NO
Oman	OM
Pakistan	PK
Panama	PA
Paraguay	PY
Peru	PE
Philippines	PH
Poland	PL
Portugal	PT
Puerto Rico	PR
Qatar	QA
Romania	RO
Russia	RU
Saudi Arabia	SA
Serbia	RS
Singapore	SG
Slovak Republic	SK
Slovenia	SI
South Africa	ZA
South Korea	KR
Spain	ES
Sri Lanka	LK
Sweden	SE
Switzerland	CH
Taiwan	TW
Thailand	TH
Trinidad and Tobago	TT
Tunisia	TN
Turkey	TR
UAE	AE
Ukraine	UA
United Kingdom	GB
Uruguay	UY
USA	US
Venezuela	VE
Vietnam	VN
Virgin Islands (British)	VG

B

APPENDIX

Usage Scenarios

This appendix section provides practical usage scenarios for many of the Access Point's key features. This information should be referenced as a supplement to the information contained within this Product Reference Guide.

The following scenarios are described:

- Configuring Automatic Updates using a DHCP or Linux BootP Server on page 631
- Configuring an IPSEC Tunnel and VPN FAQs on page 638

Configuring Automatic Updates using a DHCP or Linux BootP Server

This section provides specific details for configuring either a DHCP or Linux BootP Server to send firmware or configuration file updates to an Access Point.

The AutoUpdate feature updates the Access Point firmware and/or configuration automatically when the Access Point is reset or does a DHCP request. The update process is conducted over the LAN or WAN port depending on which server responds first to the Access Point's request for an automatic update.

The firmware is automatically updated each time firmware versions are found to be different between what is running on the Access Point and the firmware file that resides on the server. The configuration file is automatically applied when the configuration filename is found to be different between what resides on the Access Point and the filename residing on the server or when the configuration version is found to be different between what resides on the Access Point and the configuration version residing on the server.

The configuration version can be modified in the text file to cause the configuration to be applied when required. The Access Point only checks the two characters after the third hyphen (01) when making a comparison. Change the last two characters to update the configuration. The two characters can be alpha-numeric.

Windows - DHCP Server Configuration

See the following sections for information on these DHCP server configurations in the Windows environment:

- Embedded Options - Using Option 43 on page 632
- Global Options - Using Extended/Standard Options on page 633
- DHCP Priorities on page 635

Embedded Options - Using Option 43

This section provides instructions for automatic update of firmware and configuration file via DHCP using extended options or standard options configured globally.

The setup example described in this section includes:

- 1 Access Point (either an Altitude 4710 or Altitude 4750 model)
- 1 Microsoft Windows DHCP Server
- 1 TFTP Server

Note the following caveats regarding this procedure before beginning:

- Ensure the LAN Interface is configured as a DHCP Client
- If the existing and update firmware files are the same, the firmware will not get updated.

To configure the DHCP Server for automatic updates:

1 Set the Windows DHCP Server and Access Point on the same Ethernet segment.

2 Configure the Windows based DHCP Server as follows:

  a Highlight the Server Domain Name (for example, apfw.extremenetworks.com). From the *Action* menu, select *Define Vendor Classes*.

  b Create a new vendor class. For example, AP4700 Options.

  c Enter the vendor class Identifier *ExtremeAP.4700***.** Enter the value in ASCII format, the server converts it to hex automatically.

  d From the *Action* menu, select *Set Predefined Options*.

  e Add the following 3 new options under AP4700 Options class:

	Code	Data type
Access point TFTP Server IP Address (Note: Use any one option)	181 186	IP address String
Access point Firmware File Name	187	String
Access point Config File Name (Note: Use any one option)	129 188	String String

  f Highlight *Scope Options* from the tree and select *Configure Options*.

  g Go to the *Advanced* tab. From under the Vendor Class AP4700 Options, check all three options mentioned in the table above and enter a value for each option.

3 Copy the firmware and configuration files to the appropriate directory on the TFTP Server.

4 Restart the Access Point.

5 While the Access Point boots, verify the Access Point:

- Obtains and applies the expected IP Address from the DHCP Server
- Downloads both the firmware and configuration files from the TFTP Server and updates both as needed. Verify the file versions within the *System Settings* screen.

NOTE

If the firmware files are the same, the firmware will not get updated. If the configuration file name matches the last used configuration file on the Access Point or if the configuration file versions are the same, the Access Point configuration will not get updated.

Global Options - Using Extended/Standard Options

The following are instructions for automatic firmware and configuration file updates via DHCP using extended options or standard options configured globally.

The setup example described in this section includes:

- 1 Access Point (either an Altitude 4710 or Altitude 4750 model)
- 1 Microsoft Windows DHCP Server
- 1 TFTP Server.

To configure Global options using extended/standard options:

1 Set the Windows DHCP Server and Access Point on the same Ethernet segment.

2 Configure the Windows based DHCP Server as follows:

a Highlight the Server Domain Name (for example, apfw.extremenetworks.com). From the *Action* menu, select *Set Predefined Options.*

b Add the following 3 new options under *DHCP Standard Options* class:

Extended Options	Code	Data type
Access point TFTP Server IP Address (Note: Use any one option)	181 186	IP address String
Access point Firmware File Name	187	String
Access point Config File Name (Note: Use any one option)	129 188	String String

Standard Options	Code	Data type
Access point TFTP Server IP Address	66	String
Access point Firmware File Name	67	String

NOTE

If using Standard Options and the configuration of the Access Point needs to be changed, use option 129 or 188 as specified in the Extended Options table. Standard options 66 and 67 are already present in the DHCP Standard Options Class by default.

c Highlight *Scope Options* and select *Configure Options*.

d Under the *General* tab, check all 3 options mentioned within the Extended Options table and enter a value for each option.

3 Copy both the firmware and configuration files to the appropriate directory on the TFTP Server.

By default, auto update is enabled on the Access Point (since the LAN Port is a DHCP Client, out-of-the-box auto update support is on the LAN Port).

4 Restart the Access Point.

5 While the Access Point boots up, verify the Access Point:

- Obtains and applies the expected IP Address from the DHCP Server
- Downloads the firmware and configuration files from the TFTP Server and updates both as required. Verify the file versions within the *System Settings* screen.

NOTE

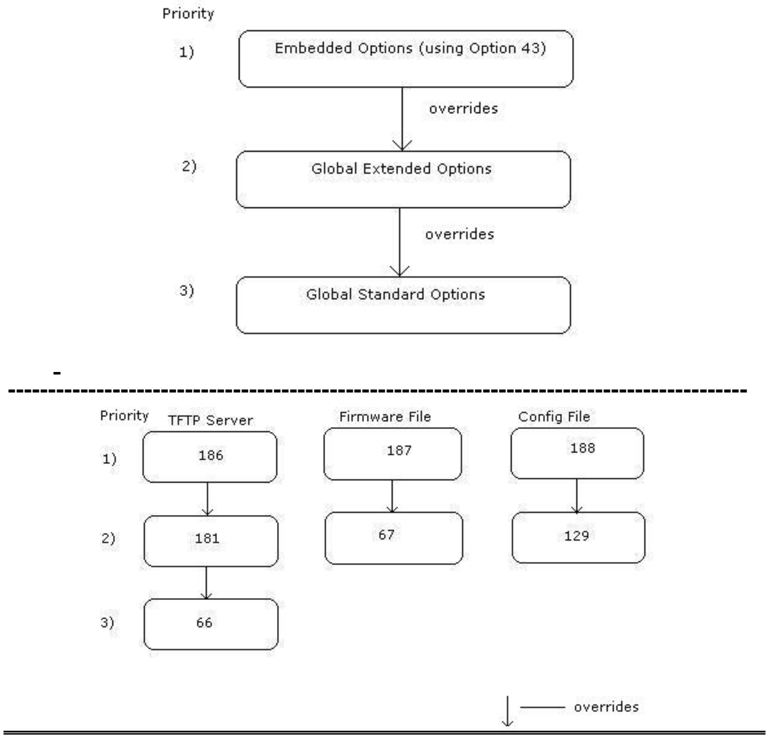
If the firmware files are the same, the firmware will not get updated. If the configuration file name matches the last used configuration file on the Access Point or if the configuration file versions are the same, the Access Point configuration will not get updated.

NOTE

The update process is conducted over the LAN or WAN port depending on which Server responds first to the Access Point's request for an automatic update.

DHCP Priorities

The following flowchart indicates the priorities used by the Access Point when the DHCP server is configured for multiple options.



If the DHCP Server is configured for options 186 and 66 (to assign TFTP Server IP addresses) the Access Point uses the IP address configured for option 186. Similarly, if the DHCP Server is configured for options 187 and 67 (for the firmware file) the Access Point uses the file name configured for option 187. If the DHCP Server is configured for embedded and global options, the embedded options take precedence.

Linux - BootP Server Configuration

See the following sections for information on these BootP server configurations in the Linux environment:

- BootP Options on page 635
- BootP Priorities on page 637

BootP Options

This section contains instructions for the automatic update of the Access Point firmware and configuration file using a BootP Server.

The setup example described in this section includes:

- 1 Access Point (either an Altitude 4710 or Altitude 4750 model)
- 1 Linux/Unix BOOTP Server
- 1 TFTP Server

To configure BootP options using a Linux/Unix BootP Server:

1 Set the Linux/Unix BootP Server and Access Point on the same Ethernet segment.

2 Configure the bootptab file (/etc/bootptab) on the Linux/Unix BootP Server in any one of the formats that follows:

Using options 186, 187 and 188:

```
AP47xx:ha=00a0f88aa6d8\    <LAN MAC Address>
   :sm=255.255.255.0\      <Subnet Mask>
   :ip=157.235.93.128\     <IP Address>
   :gw=157.235.93.2\       <gateway>
   :T186="157.235.93.250"\ <TFTP Server IP>
   :T187="apfw.bin"\       <Firmware file>
   :T188="cfg.txt":        <Configuration file>
```

Using options 66, 67 and 129:

```
AP47xx:ha=00a0f88aa6d8\    <LAN MAC Address>
   :sm=255.255.255.0\      <Subnet Mask>
   :ip=157.235.93.128\     <IP Address>
   :gw=157.235.93.2\       <gateway>
   :T66="157.235.93.250"\  <TFTP Server IP>
   :T67="apfw.bin"\        <Firmware file>
   :T129="cfg.txt":        <Configuration file>
```

Using options sa, bf and 136:

```
AP47xx:ha=00a0f88aa6d8\    <LAN MAC Address>
   :sm=255.255.255.0\      <Subnet Mask>
   :ip=157.235.93.128\     <IP Address>
   :gw=157.235.93.2\       <gateway>
   :sa=157.235.93.250\     <TFTP Server IP>
   :bf=/tftpboot/cfg.txt\  <Configuration file>
   :T136="/tftpboot/":     <TFTP root directory>
```

NOTE

The bf option prefixes a forward slash (/) to the configuration file name. The forward slash may not be supported on Windows based TFTP Servers.

3 Copy the firmware and configuration files to the appropriate directory on the TFTP Server.

By default, auto update is enabled on the Access Point (since the LAN Port is a DHCP Client, out-of-the-box auto update support is on the LAN Port).

4 Restart the Access Point.

5 While the Access Point boots, verify the Access Point:

- Sends a true BootP request.
- Obtains and applies the expected IP Address from the BootP Server.
- Downloads both the firmware and configuration files from the TFTP Server and updates them as required. Verify the file versions within the *System Settings* screen.

Whenever a configuration file is specified, the Access Point will tftp the config file, parse it and use the firmware file name in the config file.

If T136 is provided by the server, the Access Point strips off the TFTP root directory from the fully qualified configuration file name to obtain a relative file name. For example, if using bf=/opt/tftpdir/ftp/dist/ap.cfg and T136="/opt/tftpdir", the config file name is ftp/dist/ap.cfg. T136 is only used for this purpose. It is NOT used to append to the config file name or the firmware file name. If T136 is not specified, the Access Point uses the entire bf field as the config file name.

NOTE

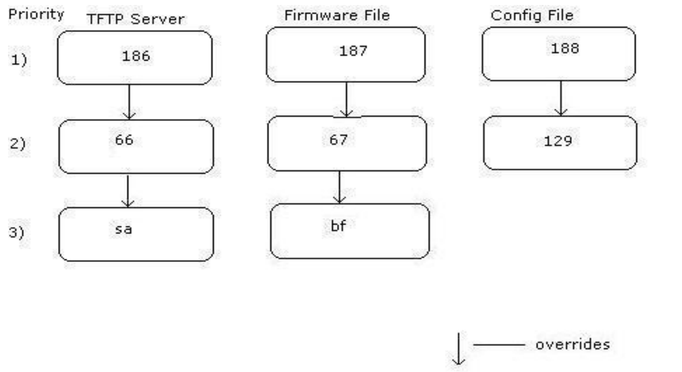
The update process is conducted over the LAN or WAN port depending on which Server responds first to the Access Point’s request for an automatic update.

NOTE

If the firmware files are the same, the firmware will not get updated. If the configuration file name matches the last used configuration file on the Access Point or if the configuration file versions are the same, the Access Point configuration will not get updated. The LAN Port needs to be configured as a BootP client. There's no BootP support on the WAN Port. The WAN supports only DHCP.

BootP Priorities

The following flowchart displays the priorities used by the Access Point when the BootP server is configured for multiple options:



If the BootP Server is configured for options 186 and 66 (to assign TFTP server IP addresses) the Access Point uses the IP address configured for option 186. Similarly, if the BootP Server is configured for options 188 and 129 (for the configuration file) the AP uses the file name configured for option 188.

Configuring an IPSEC Tunnel and VPN FAQs

The Access Point has the capability to create a tunnel between an Access Point and a VPN endpoint. The Access Point can also create a tunnel from one Access Point to another Access Point.

The following instruction assumes the reader is familiar with basic IPSEC and VPN terminology and technology.

- Configuring a VPN Tunnel Between Two Access Points on page 638
- Configuring a Cisco VPN Device on page 641
- Frequently Asked VPN Questions on page 642

Configuring a VPN Tunnel Between Two Access Points

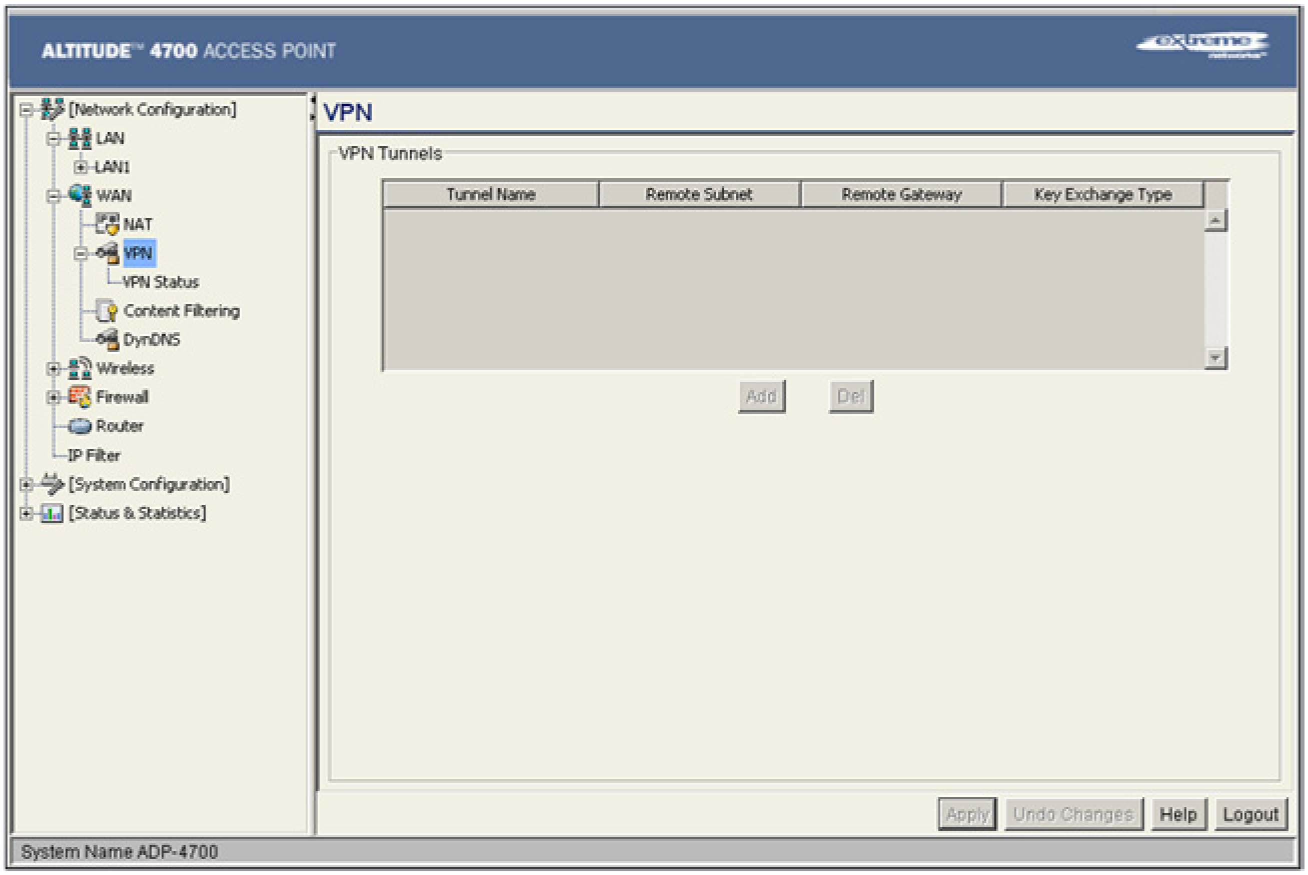
The Access Point can connect to a non-AP device supporting IPSec, such as a Cisco VPN device - labeled as "Device #2".

For this usage scenario, the following components are required:

- 1 Access Point (either an Altitude 4710 or Altitude 4750 model)
- 1 PC on each side of the Access Point’s LAN.

To configure a VPN tunnel between two Access Points:

1. Ensure the WAN ports are connected via the internet.
2. On Access Point #1, select *WAN* > *VPN* from the main menu tree.
3. Click *Add* to add the tunnel to the list.
4. Enter a tunnel name (tunnel names do not need to match).



5 Enter the WAN port IP address of AP #1 for the *Local WAN IP*.

6 Within the *Remote Subnet* and *Remote Subnet Mask* fields, enter the LAN IP subnet and mask of AP #2 /Device #2.

7 Enter the WAN port IP address of AP #2/ Device #2 for a *Remote Gateway*.

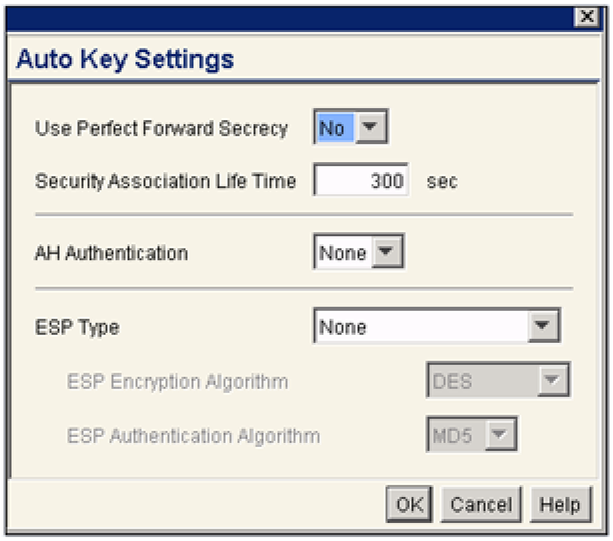
8 Click *Apply* to save the changes.

NOTE

For this example, Auto IKE Key Exchange is used. Any key exchange can be used, depending on the security needed, as long as both devices on each end of the tunnel are configured exactly the same.

9 Select the *Auto (IKE) Key Exchange* radio button.

10 Select the *Auto Key Settings* button.



Auto Key Settings

Use Perfect Forward Secrecy: No

Security Association Life Time: 300 sec

AH Authentication: None

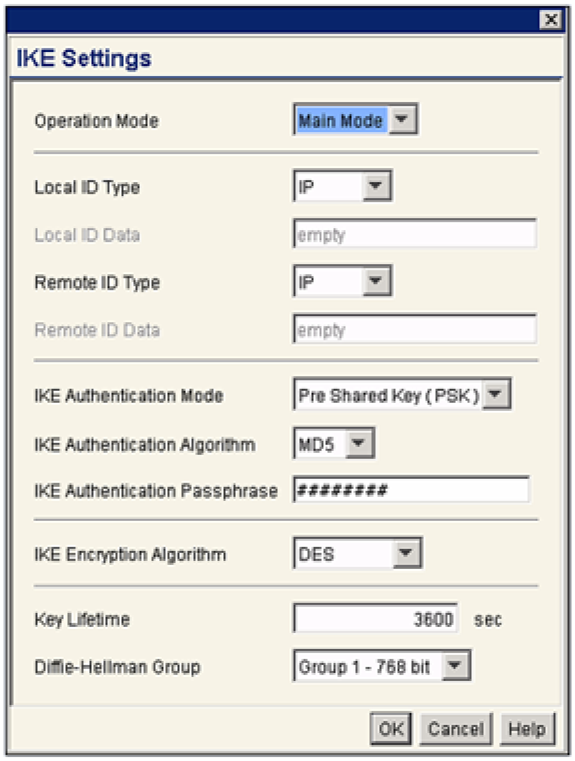
ESP Type: None

ESP Encryption Algorithm: DES

ESP Authentication Algorithm: MD5

11 For the ESP Type, select *ESP with Authentication* and use *AES 128-bit* as the ESP encryption algorithm and *MD5* as the authentication algorithm. Click *OK*.

12 Select the *IKE Settings* button.



IKE Settings

Operation Mode: Main Mode

Local ID Type: IP

Local ID Data: empty

Remote ID Type: IP

Remote ID Data: empty

IKE Authentication Mode: Pre Shared Key (PSK)

IKE Authentication Algorithm: MD5

IKE Authentication Passphrase: ########

IKE Encryption Algorithm: DES

Key Lifetime: 3600 sec

Diffie-Hellman Group: Group 1 - 768 bit

13 Select *Pre Shared Key (PSK)* from the IKE Authentication Mode drop-down menu.

14 Enter a *Passphrase*. Passphrases must match on both VPN devices.

NOTE

Ensure the IKE authentication Passphrase is the same as the Pre-shared key on the Cisco PIX device.

15 Select *AES 128-bit* as the IKE Encryption Algorithm.

16 Select *Group 2* as the Diffie-Hellman Group. Click *OK*. This will take you back to the VPN screen.

17 Click *Apply* to make the changes

18 Check the *VPN Status* screen. Notice the status displays "NOT_ACTIVE". This screen automatically refreshes to get the current status of the VPN tunnel. Once the tunnel is active, the IKE_STATE changes from NOT_CONNECTED to SA_MATURE.

19 On Access Point #2/ Device #2, repeat the same procedure. However, replace Access Point #2 information with Access Point #1 information.

20 Once both tunnels are established, ping each side of the tunnel to ensure connectivity.

Configuring a Cisco VPN Device

This section includes general instructions for configuring a Cisco PIX Firewall 506 series device.

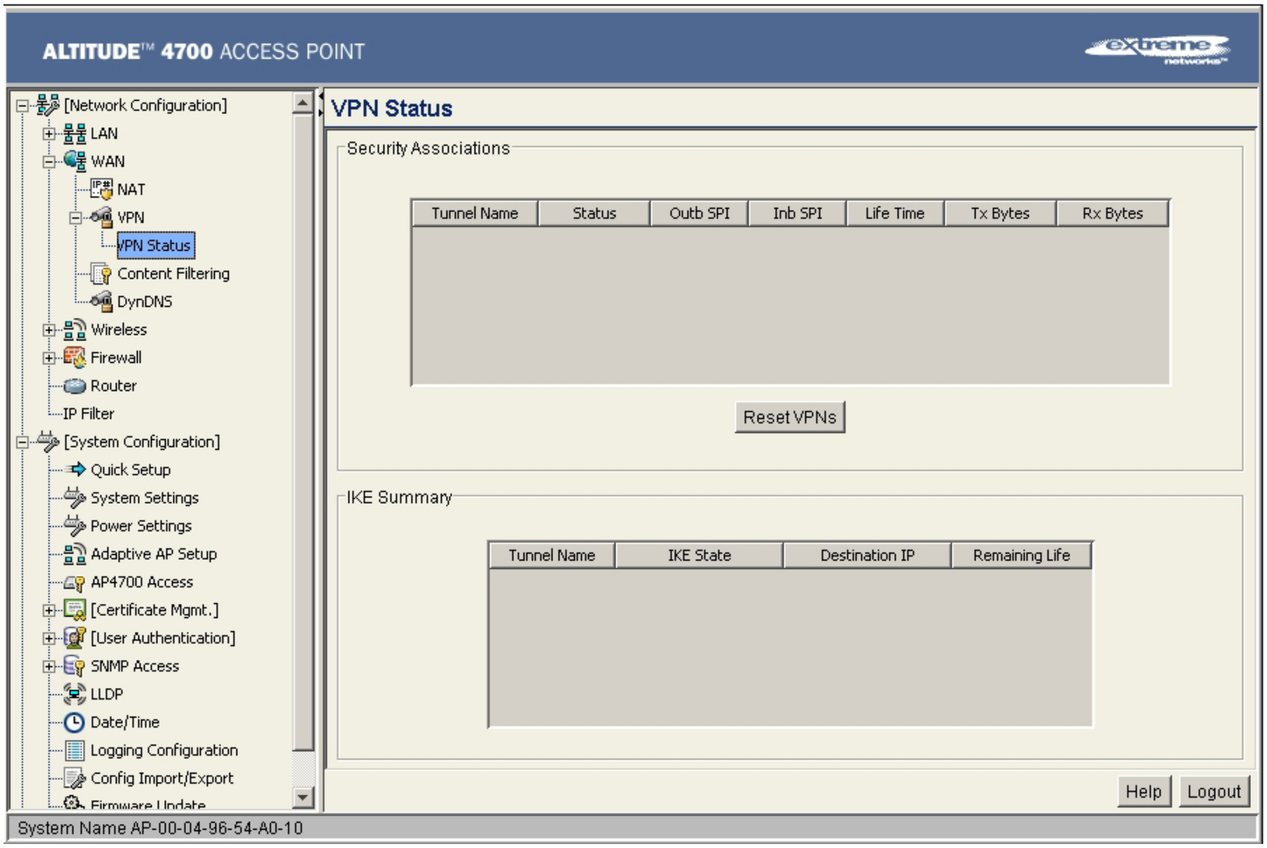
For the usage scenario described in this section, you will require the following:

- 1 Cisco VPN device
- 1 PC connected to the LAN side of the Access Point and the Cisco PIX.

NOTE

The Cisco PIX device configuration should match the Access Point VPN configuration in terms of Local WAN IP (PIX WAN), Remote WAN Gateway (Access Point WAN IP), Remote Subnet (Access Point LAN Subnet), and the Remote Subnet Mask. The Auto Key Settings and the IKE Settings on the Cisco PIX should match the Access Point Key and IKE settings.

The figure below shows how the Access Point VPN Status screen should look if the entire configuration is set up correctly once the VPN tunnel is active. The status field should display “ACTIVE”.



VPN Status

Security Associations

Tunnel Name	Status	Outb SPI	Inb SPI	Life Time	Tx Bytes	Rx Bytes

IKE Summary

Tunnel Name	IKE State	Destination IP	Remaining Life

System Name AP-00-04-96-54-A0-10

Frequently Asked VPN Questions

The following are common questions that arise when configuring a VPN tunnel.

- **Question 1: Does the Access Point IPSec tunnel support multiple subnets on the other end of a VPN concentrator?**

  Yes. The Access Point can access multiple subnets on the other end of the VPN Concentrator from the Access Point's Local LAN Subnet by:

  - Creating multiple VPN Tunnels. The AP supports a maximum of 25 tunnels.
  - When using the Remote Subnet IP Address with an appropriate subnet mask, the AP can access multiple subnets on the remote end.

  For example: If creating a tunnel using 192.168.0.0/16 for the Remote Subnet IP address, the following subnets could be accessed:

  192.168.1.x

  192.168.2.x

  192.168.3.x, etc

- **Question 2: Even if a wildcard entry of "0.0.0.0" is entered in the Remote Subnet field in the VPN configuration page, can the AP access multiple subnets on the other end of a VPN concentrator for the APs LAN/WAN side?**

  No. Using a "0.0.0.0" wildcard is an unsupported configuration. In order to access multiple subnets, the steps in Question #1 must be followed.

- **Question 3: Can the AP be accessed via its LAN interface of AP#1 from the local subnet of AP#2 and vice versa?**

  Yes.

- **Question 4: Will the default "Manual Key Exchange" settings work without making any changes?**

  No. Changes need to be made. Enter Inbound and Outbound ESP Encryption keys on both APs. Each one should be of 16 Hex characters (depending on the encryption or authentication scheme used). The VPN tunnel can be established only when these corresponding keys match. Ensure the Inbound/Outbound SPI and ESP Authentication Keys have been properly specified.

- **Question 5: Can an IPSec tunnel over a PPPoE connection be established - such as a PPPoE enabled DSL link?**

  Yes. The Access Point supports tunneling when using a PPPoE username and password.

- **Question 6: Can I setup an Access Point so clients can access both the WAN normally and only use the VPN when talking to specific networks?**

  Yes. Only packets that match the VPN Tunnel Settings will be sent through the VPN tunnel. All other packets will be handled by whatever firewall rules are set.

- **Question 7: How do I specify which certificates to use for an IKE policy from the Access Point certificate manager?**

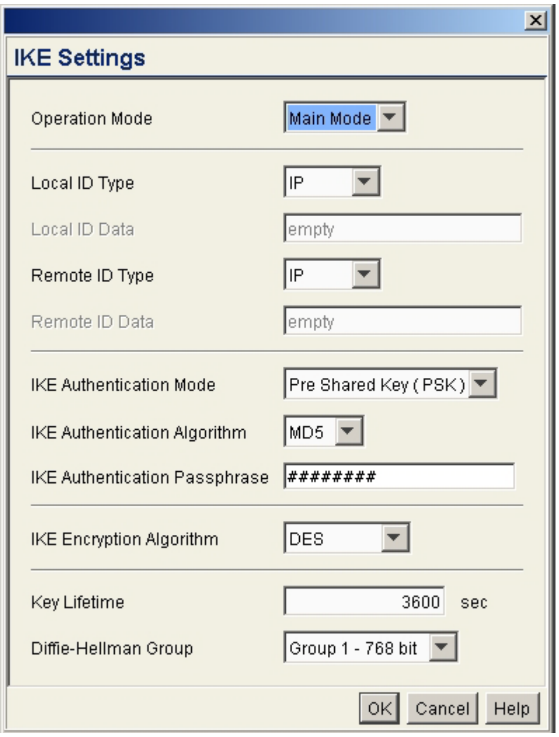
  When generating a certificate to use with IKE, use one of the following fields: *IP address*, *Domain Name*, or *Email* address. Also, make sure you are using NTP when attempting to use the certificate manager. Certificates are time sensitive.

  Configure the following on the *IKE Settings* page:

  Local ID type refers to the way that IKE selects a local certificate to use.

  - *IP*—tries the match the local WAN IP to the IP addresses specified in a local certificate.
  - *FQDN*—tries to match the user entered local ID data string to the domain name field of the certificate.
  - *UFQDN*—tries to match the user entered local ID data string to the email address field of the certificate.
  - *Remote ID type* refers to the way you identify an incoming certificate as being associated with the remote side.
  - *IP*—tries the match the remote gateway IP to the IP addresses specified in the received certificate.
  - *FQDN*—tries to match the user entered remote ID data string to the domain name field of the received certificate.

- *UFQDN*—tries to match the user entered remote ID data string to the email address field of the received certificate.



IKE Settings

Operation Mode: Main Mode

Local ID Type: IP

Local ID Data: empty

Remote ID Type: IP

Remote ID Data: empty

IKE Authentication Mode: Pre Shared Key (PSK)

IKE Authentication Algorithm: MD5

IKE Authentication Passphrase: ########

IKE Encryption Algorithm: DES

Key Lifetime: 3600 sec

Diffie-Hellman Group: Group 1 - 768 bit

- **Question 8: I am using a direct cable connection between my two VPN gateways for testing and cannot get a tunnel established, yet it works when I set them up across another network or router. Why?**

  The packet processing architecture of the Access Point VPN solution requires the WAN default gateway to work properly. When connecting two gateways directly, you don't need a default gateway when the two addresses are on the same subnet. As a workaround, point the Access Point's WAN default gateway to be the other VPN gateway and vice-versa.

- **Question 9: I have setup my tunnel and the status still says 'Not Connected'. What should I do now?**

  VPN tunnels are negotiated on an “as-needed” basis. If you have not sent any traffic between the two subnets, the tunnel will not get established. Once a packet is sent between the two subnets, the VPN tunnel setup occurs.

- **Question 10: I still can't get my tunnel to work after attempting to initiate traffic between the two subnets. What now?**

  Try the following troubleshooting tips:

  - Verify you can ping each of the remote Gateway IP addresses from clients on either side. Failed pings can indicate general network connection problems.
  - Pinging the internal gateway address of the remote subnet should run the ping through the tunnel as well. Allowing you to test, even if there are no clients on the remote end.
  - Try re-setting the shared secret password on the Access Point.

- **Question 11: My tunnel works fine when I use the LAN-WAN Access page to configure my firewall. Now that I use Advanced LAN Access, my VPN stops working. What am I doing wrong?**

  VPN requires certain packets to be passed through the firewall. Subnet Access automatically inserts these rules for you when you do VPN. Advanced Subnet Access requires these rules to be in effect for each tunnel.

  - An 'allow' inbound rule:

Scr	<Remote Subnet IP range>
Dst	<Local Subnet IP range>
Transport	ANY
Scr port	1:65535
Dst port	1:65535
Rev NAT	None

  - An 'allow' outbound rule:

Scr	<Local Subnet IP range>
Dst	<Remote Subnet IP range>
Transport	ANY
Scr port	1:65535
Dst port	1:65535
NAT	None

  - For IKE, an 'allow' inbound rule:

Scr	<Remote Subnet IP range>
Dst	<WAN IP address>
Transport	UDP
Scr port	1:65535
Dst port	500
Rev NAT	None

  These three rules should be configured above all other rules (default or user defined). When Advanced LAN Access is used, certain inbound/outbound rules need to be configured to control incoming/outgoing packet flow for IPSec to work properly (with Advanced LAN Access). These rules should be configured first before other rules are configured.

- **Question 12: Do I need to add any special routes on the Access Point to get my VPN tunnel to work?**

  No. However, clients could need extra routing information. Clients on the local LAN side should either use the Access Point as their gateway or have a route entry tell them to use the Access Point as the gateway to reach the remote subnet.

APPENDIX C

Customer Support

NOTE

Services can be purchased from Extreme Networks or through one of its channel partners. If you are an end-user who has purchased service through an Extreme Networks channel partner, please contact your partner first for support.

Extreme Networks Technical Assistance Centers (TAC) provide 24x7x365 worldwide coverage. These centers are the focal point of contact for post-sales technical and network-related questions or issues. TAC will create a Service Request (SR) number and manage all aspects of the SR until it is resolved. For a complete guide to customer support, see the *Technical Assistance Center User Guide* at:

www.extremenetworks.com/go/TACUserGuide

The Extreme Networks eSupport website provides the latest information on Extreme Networks products, including the latest Release Notes, troubleshooting, downloadable updates or patches as appropriate, and other useful information and resources. Directions for contacting the Extreme Networks Technical Assistance Centers are also available from the eSupport website at:

https://esupport.extremenetworks.com

Registration

If you have not already registered this product with Extreme Networks, you can register on the Extreme Networks website at:

http://www.extremenetworks.com/go/productregistration

Documentation

Check for the latest versions of documentation on the Extreme Networks documentation website at:

http://www.extremenetworks.com/go/documentation